# Legal Cybersecurity in the Digital Age

BY JONATHAN STRIBLING-USS, ESQ.
MEDIA DEMOCRACY FUND TECHNOLOGIST FELLOW
NEW YORK CIVIL LIBERTIES UNION

NYCLU

# Legal Cybersecurity in the Digital Age

# Legal Cybersecurity in the Digital Age

By Jonathan Stribling-Uss, Esq. Media Democracy Fund Technologist Fellow at the NYCLU

## About this Report

This report analyzes the ways in which digital communication and its attendant risks – like hacking, data breaches, and government surveillance – create acute harms for the security and confidentiality of attorney-client relationships. In the digital age attorneys cannot count on the confidentially of their communications without active digital security planning.

As this document was originally headed to publication, the emergence of the COVID-19 pandemic underscored the urgent need to shore up digital communications. The public health requirement to maintain social distance and the shift to remote work – often required by government mandate – have transformed the world's understanding of the need for secure virtual meetings. In New York at the height of the crisis, the Governor ordered all non-essential legal organizations to go completely virtual, with no in-person client meetings allowed.[1] While much of New York State has reopened, that reopening is both uncertain and subject to change. The only clear constant is that the use of digital technology for legal work is accelerating.

1 Executive Orders from the Office of the Governor: Executive order 202.6: Guidance on Executive Order 202.6: "Point 14. Professional services with extensive restrictions: Lawyers may continue to perform all work necessary for any service so long as it is performed remotely. Any in-person work presence shall be limited to work only in support of essential businesses or services; however, even work in support of an essential business or service should be conducted as remotely as possible." https://esd.ny.gov/guidance-executive-order-2026 See also *Reopening New York Summary of Office Based Work Guidelines: https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/OfficesSummaryGuidelines.pdf*

Legal professional associations in New York have not done enough to prepare for a fully digital world. Other state bar associations have responded to this crisis by offering specific ethical guidance to lawyers about how to maintain client confidentiality.[2] New York bar associations have issued general health information, and financial industry lawyers are regulated under security rules issued by the Department of Financial Services, but neither specifically address ethical guidance concerning the issue of confidentiality for attorneys generally.[3] This paper assists in filling that gap. It provides concrete, accessible steps that legal organizations, especially criminal defense lawyers, can do right now to ensure their attorney client communications are not sucked up into a government surveillance database or stolen by hackers. This report proposes a set of simple actions that attorneys and clients can take to maintain the security of online communications, as well as advocacy that attorneys can engage in within their professional organizations and with elected representatives to ensure broad and permanent ethical rules that reflect the risks of modern communication and surveillance.

Although the Covid-19 crisis has exposed this digital security gap in an alarming way, the increasing use of digital communications for client matters necessitates permanent changes to legal ethics rules. Client trust is founded on the promise of confidentiality. And for this promise to be realized in our increasingly digital age, a new generation of ethics rules is required.

---

2 Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility Formal Opinion 300 (April 10, 2020), https://www.lawsitesblog.com/wp-content/uploads/sites/509/2020/04/PBA-Formal-Opinion-2020-300-Ethical-Considerations-for-Attorneys-Working-Remotely.pdf

3 New York County Law Association, Ethics Publications: https://www.nycla.org/NYCLA/Media_and_Publications/Ethics_Opinions.aspx See also, NY City Bar Association Covid-19 response: https://www.nycbar.org/member-and-career-services/committees/coronavirus-covid-19-city-bar-response-and-resources See also NY State Dept. of Fin. Ser. *Cybersecurity requirements for financial services companies* 23 NYCRR 500 (3/1/2017) available at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf)

## About the NYCLU

The New York Civil Liberties Union (NYCLU) is the New York Affiliate of the American Civil Liberties Union (ACLU). Both organizations have been advocates for liberty and freedom in the technological age, including support for encryption, robust standards for internet privacy, the privacy of health records,[4] the security of identification documents,[5] and consumer privacy protections. The ACLU has also strongly opposed the monitoring of attorney-client communications[6] and the unlawful government surveillance of legal advocates.[7]

## I. Introduction

The digital age creates profound and uneven threats to information security. Among them are the increased surveillance and hacking of digital communications. In turn, these risks create particular barriers to ethical modern lawyering: they threaten the confidentiality of communication between lawyers and clients, which is a core underlying principle of our legal system. [8] Lawyers are obligated by professional ethics to protect the content of their communications, the nature of their legal

---

4 Corinne A. Carey & Gillian Stern, "Protecting Patient Privacy: Strategies for Regulating Electronic Health Records Exchange" New York Civil Liberties Union (3/2012), https://www.nyclu.org/sites/default/files/publications/nyclu_PatientPrivacy.pdf

5 Udi Ofer, et. al., "No Freedom Without Privacy: The REAL ID Act's Assault on Americans' Everyday Life" New York Civil Liberties Union (2/2009) https://www.nyclu.org/sites/default/files/publications/nyclu_pub_no_freedom_without_privacy.pdf

6 ACLU "Informational Privacy in the Digital Age" ACLU (2/2015) available at https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf ACLU fact sheet "Encryption: Protecting Privacy and Security" see also, G. Alex Sinha, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy,* Human Rights Watch (07/28/2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and# [https://archive.ph/pTluM]

7 ORGANIZATIONAL POLICIES, BYLAWS OF A.C.L.U, INC. Policy #518, Disclosure of ACLU Information, see also *Police Surveillance of Political Activity -- The History and Current State of the Handschu Decree. Testimony Of Arthur N. Eisenberg presented To The New York Advisory Committee To The U.S. Commission On Civil Rights*, NYCLU (May 21st, 2003) https://www.nyclu.org/en/publications/testimony-police-surveillance-political-activity-history-and-current-state-handschu [https://archive.fo/uVjMu]

8 *See, e.g., Upjohn Co. v. United States*, 449 U.S. 383, 389, 101 S.Ct. 677, 682, 66 L.Ed.2d 584 (1981) (The "full and frank communication between attorneys and their clients ... promote[s] broader public interests in the observance of law and the administration of justice.").

investigations, and often even the fact that they are communicating with a particular individual. Unfortunately, as a group, lawyers have failed to update their Model Rules of Professional Conduct to match society's technical advancements.[9] Without taking immediate steps to secure their digital legal communications, attorneys risk losing client trust and breaching their duties to clients.

Today, only attorneys that take active steps to recognize and account for the risks of our increasingly online communications can truly comply their duty of confidentiality. Clients must demand more robust and verifiable confidential systems from their attorneys, and lawyers should provide such systems by default.[10] But lawyers should not be left to revamp ethical standards on their own. Attorney professional organizations must also see digital security threats as threats to attorney ethics and act accordingly. Securing justice in the information age requires updated standards and regulations to protect client confidences. Indeed, other professional sectors have come to this recognition faster than lawyers. For example, the financial services industry is now required to engage in basic digital security in New York State, like two-factor authentication and encryption.[11] It would be deeply unjust for only clients in the financial sector to be ensured meaningful confidentiality – other legal clients have no lesser claim to this right. The regulations currently create a two tier system of law, where wealthy people connected to the finance industry can expect demonstrable security from their attorney client communications, while everyone else is left to insecurely hope that their attorney hasn't been hacked yet. Rules that govern the practice of law must recognize and account for ways in which digital risks are impacting the profession – to ensure a legal system that is just, secure, and effective.

---

9 Model Rules of Prof'l Conduct R. 1.6, cmt. 16 (2016).

10 *Jason Shore and Coinabul, LLC v. Johnson & Bell, Ltd.*, Docket No.: 1:16-cv-or04363 MIS/SES , N.D. Il., filed April 15, 2016, https://law.justia.com/cases/federal/district-courts/illinois/ilndce/1:2016cv04363/325450/56/

11 NY State Dept. of Fin. Ser. *Cybersecurity requirements for financial services companies* 23 NYCRR 500 (3/1/2017) available at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf Section 500.12 and Section 500.15

These rules become all the more critical in a crisis like the one created by the novel COVID-19 pandemic. Not only has the health care response to the virus been bottlenecked by a lack of uniform confidentiality standards, but as part of their pandemic response many state governments have issued stay at home orders requiring non-essential business, including legal offices, to work remotely.[12] At the height of the pandemic in New York, the Governor's Executive Order 202.6 required all non-essential legal offices to use digital processes for nearly all of their basic operations.[13] NY State Bar Associations have issued general health information to assist lawyers in the pandemic but, unlike other state bar associations, they have not specifically addressed ethical guidance concerning the issue of confidentiality during the response to COVID-19.[14]

Every client deserves the right to secure, confidential, and effective legal representation. This report demonstrates how attorneys can accomplish this goal with little cost or disruption, in a way that saves resources and time in the long term. Further, it will outline how attorneys should themselves become advocates within their professional associations and communities for broad standards that ensure that clients' rights are protected even in a fully digital world.

---

12 Sarah Kliff and Margot Sanger-Katz, *Bottleneck for U.S. Coronavirus Response: The Fax Machine,* The N.Y. Times (7/13/2020), https://www.nytimes.com/2020/07/13/upshot/coronavirus-response-fax-machines.html[https://archive.fo/HQPLz ] see also PwC's US Remote Work Survey, *When everyone can work from home, what's the office for?*, PWC, (6/25/20) https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

13 Executive Orders from the Office of the Governor: Executive order 202.6: Guidance on Executive Order 202.6: "Point 14. Professional services with extensive restrictions: Lawyers may continue to perform all work necessary for any service so long as it is performed remotely. Any in-person work presence shall be limited to work only in support of essential businesses or services; however, even work in support of an essential business or service should be conducted as remotely as possible." https://esd.ny.gov/guidance-executive-order-2026 See also https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/OfficesSummaryGuidelines.pdf. See also NY Governor, *No. 202 Executive Order: Declaring a Disaster Emergency in the State of New York*, https://www.governor.ny.gov/news/no-202-declaring-disaster-emergency-state-new-york

14 Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility Formal Opinion 300,(April 10, 2020), https://www.lawsitesblog.com/wp-content/uploads/sites/509/2020/04/PBA-Formal-Opinion-2020-300-Ethical-Considerations-for-Attorneys-Working-Remotely.pdf

## II. Threats: How New Technologies Harm the Attorney-Client Relationship

Data security is at risk globally, domestically, and here in New York State. The World Economic Forum has identified the lack of cybersecurity as one of the top ten threats to global security, writ large.[15] The US intelligence community has asserted that cybersecurity is one of the top threats to the world in its "worldwide threat assessment" for the past 3 years.[16] These threats have real-world economic consequences. Each year for the past 13 years IBM and the Ponemon Institute have analyzed the cost associated with data breaches of less than 100,000 records.[17] They found a nearly 10 percent net increase over 5 years of the study, where the average cost of a data breach was $3.86 million in the 2018 study, up from $3.50 million in 2014.[18]

The legal profession is no stranger to these threats. More than 100 US law firms have reported data breaches to authorities since 2014. [19] In 2018, the law firm of Mossack Fonseca, the world's fourth largest provider of offshore financial services, abruptly shut its doors after falling victim to a breach of more than 11.5 million leaked files spanning nearly 40 years of data from its more than 35 locations around

---

15 *The Global Risks Report 2019, 14th Edition,* World Economic Forum (2019) pg, 8, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf, see also *The Global Risks Report 2016, 11th Edition,* World Economic Forum (2016), http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf, see also, *The Global Risk Report 2017, 12th Edition,* World Economic Forum (2017) http://www3.weforum.org/docs/GRR17_Report_web.pdf

16 Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community" (2019) https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf see also Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community" (2017) https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

17 These numbers do not even include the 16 breaches in 2017 involving more than 1 million records. These mega breaches are estimated to have an average cost that range from $40 million dollars for 1 million compromised records to $350 million dollars as an estimate for breaches of 50 million records.IBM, *IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses*, https://newsroom.ibm.com/2018-07-10-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

18 IBM, *IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses*, https://newsroom.ibm.com/2018-07-10-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

19 Christine Simmons, Xiumei Dong and Ben Hancock, *More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse,* Law.com (10/15/19) https://www.law.com/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse

the globe.[20] Such breaches have occurred here in New York as well. In New York State, the number of unique law firm data breaches doubled from 2017 to 2018, impacting nearly 1,500 individuals.[21] In a recent action in Manhattan Supreme Court, a New York couple alleged that over $1.9 million of their money had been stolen because of their real estate lawyer's negligence in failing to encrypt her communications, which allowed cyber criminals to read and intercept the lawyers' email communications, leading to the theft of client funds. [22]

Threats to data "security" consist of far more than one-off data breaches or hacks. Intelligence agencies create organized systems that *ensure* digital communications are intercepted, that digital products are intentionally rife with backdoors (see also section on Vulnerabilities Equities Process, *infra*), and that evidence of cybersurveillance will be all but impossible to sniff out in criminal cases. And attorneys should be concerned even if they don't view themselves as representing clients likely in the crosshairs of government surveillance; as noted below, these systems of surveillance sweep up an immense of volume of records of targeted groups and individuals – but an even greater volume of communications comes from those incidentally collected by this government mass surveillance. Every attorney must con-

---

20 Will Fitzgibbon, *Panama Papers law firm Mossack Fonseca closes its doors,* The International Consortium of Investigative Journalists (ICIJ) (3/14/2018), https://www.icij.org/investigations/panama-papers/panama-papers-law-firm-mossack-fonseca-closes-doors/ see also Hans Leyendecker et al. *The Firm,* Süddeutsche Zeitung GmbH (last visited 2/26/2019), https://panamapapers.sueddeutsche.de/articles/56febf8da1bb8d3c3495adec/ see also Nick Hopkins & Helena Bengtsson, *What are the Paradise Papers and what do they tell us?* The Guardian (11/5/2017), https://www.theguardian.com/news/2017/nov/05/what-are-the-paradise-papers-and-what-do-they-tell-us [https://archive.vn/kjzLr]

21 Fragomen Data Breach NY https://www.documentcloud.org/documents/6442849-Fragomen-Data-Breach-NY.html Black Rome Data Breach: https://www.documentcloud.org/documents/6442845-BlankRome-Data-Breach-NY.html Johnson Hearn Data Breach: https://www.documentcloud.org/documents/6434426-JohnsonHearn-Data-Breach-NY.html Jenner Data Breach NY: https://www.documentcloud.org/documents/6442859-Jenner-Data-Breach-NY.html GaleMcAllister Data Breach: https://www.documentcloud.org/documents/6434411-GaleMcAllister-Data-Breach-NY.html Dawson Law Data Breach: https://www.documentcloud.org/documents/6434412-DawsonLaw-Data-Breach-NY.html

22 *Robert Millard and Bethany Millard v. Patricia L. Doran*, Supreme Court of the State of New York, County of New York, Index No.: 153262/2016, filed 4/18/2016, https://iapps.courts.state.ny.us/nyscef/ViewDocument?docIndex=DwYoLtNofB3D5sp/shG_PLUS_Aw See also, Kavita Iyer, *This couple sued their lawyer after hackers stole $1.9 million from them,* Techworm (4/20/2016) https://www.techworm.net/2016/04/couple-sued-lawyer-hackers-stole-1-9-million.html

sider how these systems impact their ability to provide truly confidential legal counsel. Below, we review each system in turn: mass surveillance, the vulnerabilities equities process, and parallel construction.

### II. a. Government Mass Surveillance

Government mass electronic surveillance seriously threatens the integrity of legal communications in the United States and around the world.[23] Mass surveillance is defined by the UN as a situation in which "states with high levels of Internet penetration can…gain access to the telephone and e-mail content of an effectively unlimited number of users and maintain an overview of Internet activity associated with particular websites." [24] Under these NSA Mass Surveillance programs—ostensibly sold to the public as a mechanism to monitor terrorists—the U.S. Government has taken privileged information from U.S. attorneys and used it to their clients' disadvantage.[25] The US government's current mass surveillance programs were revealed in documents provided by NSA whistleblower Edward Snowden.[26] The documents show that the National Security Agency (NSA) maintains a system of global mass surveillance that involves "collection directly from the servers" of nearly all large US internet companies, such as Microsoft, Yahoo, Google, Fa-

---

23 James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y.Times (2/15/2014), http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html [https://archive.ph/6jVlI] see also James R. Silkenat, *Re: Preservation of Attorney-Client Privilege for U.S. Law Firms and their Overseas Clients*, American Bar Association, https://www.scribd.com/document/208843067/ABA-Letter-to-NSA

24 The UN reports that in a system of "mass surveillance, all of this is possible without any prior suspicion related to a specific individual or organization." See also, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *Promotion and protection of human rights and fundamental freedoms while countering terrorism,* United Nations General Assembly (9/23/2014) (by Ben Emmerson) Available at http://www.ccdcoe.com/uploads/2018/11/UN-140923-HumanRightsTerrorism.pdf See also [https://archive.ph/4ownq]

25 James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y.TIMES (2/15/2014), http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html [https://archive.ph/6jVlI]

26 The Snowden Document Search aims to provide a comprehensive, easy-to-use search that draws upon all text from available Snowden documents: https://search.edwardsnowden.com/ See also: Surveillance without Borders a resource which illustrates how surveillance is being carried out around the world based on the Snowden revelations: http://surveillancewithoutborders.com/

cebook, YouTube, Skype, AOL, and Apple (through the codenamed PRISM program).[27] It also consists of taps on the fiber optic cables of most internet infrastructure companies, such as AT&T (through the codenamed STORMBREW, FAIRVIEW, BLARNEY and OAKSTAR upstream programs).[28] As well as a system to provide long term storage of collected data nearly 1000 times larger than the data of the whole internet, through the Utah Data Center in Bluffsdale, Utah[29] and near real time searching of the resulting collected data (through the codenamed XKEYSCORE program).[30]

The NSA shares full database access with the intelligence agencies of four other governments: the UK, Canada, Australia, and New Zealand, which collectively refer to themselves as "The Five Eyes." The Five Eyes' security agencies have

27Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian (6/7/2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [http://archive.fo/XjWIf]

28 Craig Timberg, *NSA slide shows surveillance of undersea cables,* The Washington Post (7/10/2013), https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html [http://archive.md/QD624]

29 James Bamford, The NSA Is Building the Country's Biggest Spy Center (Watch What You Say), Wired (3/15/2012) https://www.wired.com/2012/03/ff-nsadatacenter/ / [http://archive.md/4Is3H]

30 Glenn Greenwald, XKeyscore: NSA tool collects 'nearly everything a user does on the internet' The Guardian (7/31/2013) https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

developed strategic priorities for targeting certain groups, including: Muslim leaders of all types,[31] "radicalizers," generally,[32] Palestinian leaders,[33] the "human network" associated with Wikileaks,[34] anyone searching for privacy tools on the internet,[35] computer network operators,[36] drug dealers,[37] presidents,[38] bank officials,[39]

31 Glenn Greenwald & Murtaza Hussai, *Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On* The Intercept (7/9/2014) https://theintercept.com/2014/07/09/under-surveillance/ [https://archive.fo/oeeV7]
32 Glenn Greenwald et al., *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers',* The Huffington Post (11/26/2013), [https://archive.fo/ASMrq]
33 Glenn Greenwald, *No Place to Hide*, (Metropolitan Books 2014) pg. 114-124 *accessible at* https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [http://archive.fo/t24xg]
34 Glenn Greenwald & Ryan Gallagher, *Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters,* The Intercept (2/18/2014) https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/ [https://archive.fo/rmGkN]
35 Kim Zetter, *The NSA Is Targeting Users of Privacy Services, Leaked Code Shows*, Wired (7/3/2014) https://www.wired.com/2014/07/nsa-targets-users-of-privacy-services/ [https://archive.fo/WQXpS] see also The Intercept, *Discovery SIGINT Targeting Scenarios and Compliance*, The Intercept (2/18/2014) https://theintercept.com/document/2014/02/18/discovery-sigint-targeting-scenarios-compliance/
36 Loek Essers, *Chaos Computer Club bolsters NSA spying complaint with Tor snooping evidence,* IDG News Service (*7/17/2014)*https://www.computerworld.com.au/article/550288/chaos_computer_club_bolsters_nsa_spying_complaint_tor_snooping_evidence/ [https://archive.fo/iAsYT]
37 SID Today, *The 'Dope' on the NSA-DEA Relationship*, The Intercept (9/13/2017), https://search.edwardsnowden.com/docs/TheDopeontheNSA-DEARelationship2017-09-13_nsadocs_snowden_doc [https://archive.fo/AL8M9]
38 Kim Zetter, *NSA Secret Database Ensnared President Clinton's Private E-mail,* Wired (6/17/2009) www.wired.com/2009/06/pinwale [https://archive.fo/LyCPk] see also Glenn Greenwald, *No Place to Hide*, pg 159-167 (Metropolitan Books 2014) accessible at https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [http://archive.fo/t24xg] see also Glenn Greenwald et al. *Letter about NSA spying on economic summits,* Epoca news (2/08/2013) http://epoca.globo.com/tempo/noticia/2013/08/carta-em-que-o-atual-bembaixadorb-americano-no-brasil-bagradece-o-apoio-da-nsab.html [https://archive.fo/Zhflu]
39 Gregor Peter Schmitz, *EU Parliament Furious about NSA Bank Spying*, Der Spiegel http://www.spiegel.de/international/europe/nsa-spying-european-parliamentarians-call-for-swift-suspension-a-922920.html [https://archive.fo/XZJkE]

the UN,[40] people creating intellectual property,[41] and protestors during the 2004 RNC and DNC conventions.[42]

People that the NSA views as "radicalizers" have been targeted for "reputational" attacks for their behavior on the internet, like online promiscuity, or even simply because one "publishes articles without checking facts."[43] Internal memos make it clear that the NSA views these targeted people, some of whom are U.S. citizens, as "radicalizers" specifically because of their political speech; for visibly and influentially making arguments like "the U.S. brought the 9/11 attacks on itself."[44]

The "Five" in "Five Eyes" shouldn't be taken too literally – these governments often share full database access with even more governments. There were nearly 20 governments listed as "partners" in 2012. For example, in 2012, Saudi Arabia and Israel had signed memoranda of understanding allowing unrestricted searching of

---

40 Glenn Greenwald, *No Place to Hide*, pg 159-167 (Metropolitan Books 2014) *accessible at* [http://archive.fo/t24xg] see also Edward Moyer, *NSA spied on EU antitrust official who sparred with US tech giants*, CNET (12/20/2013) http://www.cnet.com/news/nsa-spied-on-eu-antitrust-official-who-sparred-with-us-tech-giants/ [https://archive.fo/WdjA8] see also Mark Hosenball, *Obama halted NSA spying on IMF and World Bank headquarters*, Reuters (10/31/2013) https://www.reuters.com/article/us-usa-security-imf/obama-halted-nsa-spying-on-imf-and-world-bank-headquarters-idUSBRE99U1EQ20131031 [https://archive.fo/TgqDD] see also Jonathan Watts, *NSA accused of spying on Brazilian oil company Petrobras*, The Guardian (9/9/2013), https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras [https://archive.fo/qZvx7]

41 Glenn Greenwald, *The U.S. Government's Secret Plans to Spy for American Corporations*, The Intercept (9/5/2014) https://theintercept.com/2014/09/05/us-governments-plans-use-economic-espionage-benefit-american-corporations/ [http://archive.fo/ZDzxs]

42 SID Today, *NSA Provides Un-'conventional' Support,* The Intercept (4/24/2017) https://search.edwardsnowden.com/docs/NSAProvidesUn-conventionalSupport2017-04-24_nsadocs_snowden_doc [https://archive.fo/Nxg3D] see also Glenn Greenwald, *No Place to Hide*, (Metropolitan Books 2014) pg. 114-124 *accessible at* https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [http://archive.fo/t24xg]

43 Glenn Greenwald et al., *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers',* The Huffington Post (11/26/2013), [https://archive.fo/ASMrq] see also Kim Zetter, *NSA Secret Database Ensnared President Clinton's Private E-mail,* Wired (6/17/2009) https://www.wired.com/2009/06/pinwale/ [https://archive.fo/LyCPk] see also Glenn Greenwald, *No Place to Hide*, pg 159-167 (Metropolitan Books 2014) *accessible at* https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [http://archive.fo/t24xg] see also Barton Gellman et al., *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, The Washington Post (07/05/2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [https://archive.ph/Cow3K] see also Barton Gellman, *NSA broke privacy rules thousands of times per year, audit finds*, The Washington Post, www.washingtonpost.com/world/national-security/nsa-broke-privacy-rulesthousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html [https://archive.fo/LuKlh]

44 Glenn Greenwald, *No Place to Hide*, pg 159-167 (Metropolitan Books 2014) *accessible at* https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [https://archive.fo/t24xg]

Five Eyes databases, including XKeyscore, one of the NSA's most wide ranging and intrusive search tool.[45] And private actors feed into government surveillance databases as well: nearly all U.S. based technology companies, including Apple, Facebook, Google, and Microsoft, are part of the ongoing PRISM program.[46]

Released NSA documents make it clear that an increasing number of governments, including the "Five Eyes", are engaged in this sort of indiscriminate mass surveillance of electronic communications throughout the globe.[47]

This government surveillance has even involved taking privileged information from U.S. attorneys and using it against their clients.[48] For example, the NSA illegally obtained privileged and confidential information from Mayer Brown, a major Chicago-based law firm representing the government of Indonesia in trade negotiations with the US Government. The NSA was able to access the negotiation posture of the Indonesian government, including what Indonesia would or wouldn't accept in the negotiations. The NSA shared this critical information with U.S. government negotiators who used it against Mayer Brown in those negotiations.[49] But even attorneys who don't represent anyone on the capacious list of "radicalizers"

---

45 Morgan Marquis-Boire, Glenn Greenwald, and Micah Lee, *XKEYSCORE: NSA's Google for the World's Private Communications,* The Intercept (7/1/2015), https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/ [https://archive.is/8y9Yq] see also, Glenn Greenwald, *No Place to Hide*, pg. 130-137 (Metropolitan Books 2014) *accessible at* https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [http://archive.fo/t24xg] see also Kurt Opsahl and Mark Rumold, *Reassured by NSA's Internal Procedures? Don't Be. They Still Don't Tell the Whole Story.* The EFF (6/21/2013) https://www.eff.org/deeplinks/2013/06/recently-revealed-nsa-procedures-likely-ones-found-unconstitutional-fisa-court, see also Ryan Gallagher, *The Surveillance Engine: How the NSA Built Its Own Secret Google*, The Intercept (08/25/2014), https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/ [https://archive.fo/q3fl6] see also Morgan Marquis-Boire, Glenn Greenwald, and Micah Lee, *Behind the Curtain: A look at the inner workings of the NSA's XKEYSCORE,* The Intercept (7/2/2015), https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/ [https://archive.is/R7LVu]

46 Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian (6/7/2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [http://archive.fo/XjWIf]

47 Glenn Greenwald, *No Place to Hide*, pg 77-86 (Metropolitan Books 2014) accessible at https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [http://archive.fo/t24xg]

48 James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y.TIMES (2/15/2014), http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html [https://archive.ph/6jVlI]

49 James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y.TIMES (2/15/2014), http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html [https://archive.ph/6jVlI]

above, or don't represent foreign entities in trade negotiations, are not safe from the U.S. government's surveillance apparatus. When the Washington Post analyzed information used in twenty two thousand leaked NSA surveillance reports, 89% of the information was from those who were associates of the targeted individuals, while only 11% was from the individuals actually designated as NSA targets.[50]

Because of this mass collection structure, it is virtually certain that legally privileged and confidential information has been and will be compromised in the normal course of unsecured digital attorney-client communication. The NSA has no filtering procedure for privileged attorney-client information.[51] Prosecutors have initiated investigations of clients based on this illegal electronic dragnet information (see also section on Parallel Construction, *infra*).[52] Currently it is unclear how many thousands of cases may involve this type of illegal evidence.[53] This mass surveillance also extends into the physical world with the U.S. Postal Service imaging the front and back of every piece of U.S. mail and providing the FBI with warrantless access to the images.[54] But clearly state governments are also not immune from mass collection of privileged information. Privileged and confidential attorney-client

---

50 Barton Gellman et al., *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, The Washington Post (7/5/2014) https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [https://archive.fo/Cow3K]

51 Nicolas Niarchos, *Has the NSA Wiretapping Violated Attorney-Client Privilege?,* The Nation (2/4/2014), http://www.thenation.com/article/178225/has-nsa-wiretapping-violated-attorney-client-privilege [http://archive.md/EdSzO]

52 John Shiffman & Kristina Cooke, *U.S. directs agents to cover up program used to investigate Americans*, Reuters (8/5/2013), https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805 [https://archive.fo/3OMgV]

53 Glenn Greenwald et al, *Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On,* The Intercept (7/9/2014), https://firstlook.org/theintercept/article/2014/07/09/under-surveillance/ [http://archive.fo/WAu7q] see also Glenn Greenwald, *No Place to Hide*, , Pg 159-167 (Metropolitan Books 2014) *accessible at* https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [http://archive.fo/t24xg] see also Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, The Intercept (11/30/2017) https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/ [https://archive.fo/NeIcP]

54 John Napier Tye, *Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans,* www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html see also Steven Melendez, *Suspicious packages spotlight vast postal surveillance system,* Fast Company (10.25.18), https://www.fastcompany.com/90257308/suspicious-packages-spotlight-vast-postal-surveillance-system-mail-covers [https://archive.ph/oxhC7]

communication is illegally being recorded as a matter of course by contractors working for the government, like the telephone system contractor Securus.

Securus is hired by state governments to manage calls to incarcerated people, including attorney-client communications. Securus's database was hacked and leaked to journalists.[55] It included more than 70 million individual phone calls by incarcerated people, placed to 1.3 million unique phone numbers over a 2 1/2-year period with records from at least 57,000 calls made by detainees to lawyers, including full voice calls, which attorneys confirmed had been set up in advance with law enforcement authorities to be privileged and confidential.[56]

This government mass surveillance has a chilling effect on clients whose legal matters are adversarial to the government. Clients have difficulty trusting attorneys enough to approach them.[57] It has made it far more likely that attorneys, no matter who their clients are, will have their clients' information and confidences read by others. Fortunately, there is a simple, effective solution that can prevent these harms of government surveillance: properly authenticated uniform end to end encryption of internal networks. Modern encryption is the mathematical scrambling of data so that it is only readable by the intended parties.

---

55 *Not So Securus,* The Intercept (11/11/2015) https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/ [https://archive.ph/MHC2m]

56 Jordan Smith, *Securus Settles Lawsuit Alleging Improper Recording of Privileged Inmate Calls,* The Intercept, (03/16/2016) https://theintercept.com/2016/03/16/securus-settles-lawsuit-alleging-improper-recording-of-privileged-inmate-calls/ [https://archive.fo/spdNU] see also Jordan Smith & Micah Lee, *Not So Securus,* The Intercept (11/11/2015) https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/ [https://archive.ph/MHC2m] see also Jordan Smith & Micah Lee, *Not So Securus: Part 2 Lawyers Speak Out About Massive Hack of Prisoners' Phone Records*, The Intercept, (12/02/2016) https://theintercept.com/2016/02/12/not-so-securus-lawyers-speak-out-about-massive-hack-of-prisoners-phone-records/ [https://archive.ph/4ibkz]

57 G. Alex Sinha, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy,* Human Rights Watch (07/28/2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and# [https://archive.ph/pTluM]

Proper encryption can keep clients' emails from being read by PRISM or XKeyscore. Proper encryption would have prevented Mossack Fonseca's catastrophic client failure.[58] Proper encryption would likely have prevented a lawsuit alleging the theft of client funds from a NY attorney.[59] The Ponemon Institute found that an organization's extensive use of encryption can cut the average cost of a data breach from $148 to $13 per capita compromised record.[60] Professional ethics opinions have begun to recognize this reality and urged the use of encrypted communications systems in many instances.[61] But they have not gone far enough, and New York is still behind the curve. For more information about how to import proper encryption into your legal practice, *see infra* at, The Duty to Encrypt at Page 23.

## II. b. The Vulnerabilities Equities Process

The U.S. government's Vulnerabilities Equities Process (VEP) is a set of guidelines used by government agencies to determine when to inform the public about security vulnerabilities in software and hardware.[62] The government asserts

---

58 Will Fitzgibbon, *Panama Papers law firm Mossack Fonseca closes its doors,* The International Consortium of Investigative Journalists (ICIJ) (3/14/2018), https://www.icij.org/investigations/panama-papers/panama-papers-law-firm-mossack-fonseca-closes-doors/ see also Hans Leyendecker et al. *The Firm,* Süddeutsche Zeitung GmbH (last visited 2/26/2019), https://panamapapers.sueddeutsche.de/articles/56febf8da1bb8d3c3495adec/ see also Nick Hopkins & Helena Bengtsson, *What are the Paradise Papers and what do they tell us?* The Guardian (11/5/2017), https://www.theguardian.com/news/2017/nov/05/what-are-the-paradise-papers-and-what-do-they-tell-us

59*Robert Millard and Bethany Millard v. Patricia L. Doran*, Supreme Court of the State of New York, County of New York, Index No.: 153262/2016, filed 4/18/2016, https://iapps.courts.state.ny.us/nyscef/ViewDocument?docIndex=DwYoLtNofB3D5sp/shG_PLUS_Aw See also, Kavita Iyer, *This couple sued their lawyer after hackers stole $1.9 million from them,* Techworm (4/20/2016) https://www.techworm.net/2016/04/couple-sued-lawyer-hackers-stole-1-9-million.html

60 Larry Ponemon, *Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT,* Security Intelligence (7/11/2018), https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ [https://archive.fo/Yt83E] see also National Small Business Association, *2013 Small Business Technology Survey,* http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf (9/2013) [http://archive.fo/6TMIE] see also Verizon, *Data Breach Investigations Report 2015,* https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/data-breach-investigation-report_2015.pdf [http://archive.fo/IhlQT]

61 The Professional Ethics Committee for the State Bar of Texas, Opinion No. 648 (2015) (encryption of email may be required*)* available at https://www.law.uh.edu/libraries/ethics/opinions/601-700/EO648.pdf, ABA Ethics Opinion 477 (5/11/2017) (encryption may be required) *available at* https://www.americanbar.org/content/dam/aba/images/abanews/FormalOpinion477.pdf

62 Electronic Privacy Information Center, *Vulnerabilities Equities Process*, (last accessed 4/17/19) accessible at : https://epic.org/privacy/cybersecurity/vep/

that it must *maintain* failures in key information technology products so that the government may gain access to many types of proprietary software and encryption systems (often called "backdoors").[63] What this means for attorneys is that all private propriety software is a black box – and intentionally kept that way by the government – that could, and by design is likely to, include serious vulnerabilities that risk the security of attorney-client communications.[64] In order to maintain purposely broken technology for surveillance purposes the NSA put backdoors in some proprietary encryption, including the encryption that attempted to secure Skype calls.[65] One way the NSA did this was by paying $10 million to an encryption manufacturer, named RSA, to weaken the math that secured its encryption.[66] The NSA also created a section of the National Standardization Board for Encryption within the U.S. National Institute of Standards and Technology (NIST) that would take encryption programs and insert a backdoor into the product, which would allow the NSA to guess the outcome of otherwise random code construction.[67]

---

63 United States, White House Office. *Vulnerabilities Equities Policy and Process for the United States Government* White House Office (11/15/2017) https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF see also Sam Biddle, *The NSA Leak Is Real, Snowden Documents Confirm,* The Intercept (8/19/2016) https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/

64 Proprietary software, also referred to as "closed source" or "non-free" software, includes copyright terms that maintain intellectual rights to the source code to someone other than the user. These exclusive rights over the software allow the owner to restrict use, or modification of source code. see also Michael Riley, *U.S. Agencies Said to Swap Data With Thousands of Firms,* Bloomberg (6/14/2013), https://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms [https://archive.md/6iyOs] see also SPIEGEL Staff, *Prying Eyes Inside the NSA's War on Internet Security,* DER SPIEGEL (12/28/2014) http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [https://archive.li/KzF31]

65 Glenn Greenwald, et al, *Microsoft handed the NSA access to encrypted messages,* The Guardian (7/12/2013) https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data See also Glenn Greenwald, et al, *Revealed: how US and UK spy agencies defeat internet privacy and security*, The Guardian (9/6/2013), https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [http://archive.fo/960QN]

66 Joseph Menn, *Exclusive: Secret contract tied NSA and security industry pioneer,* Reuters (12/20/2013), http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 [http://archive.fo/f6qPI]

67 Nicole Perlroth et al. *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y.TIMES (2/15/2014), https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html [https://archive.fo/DyVgN] see also Kim Zetter, *New Discovery Around Juniper Backdoor Raises More Questions About the Company,* Wired (1/8/2016), https://www.wired.com/2016/01/new-discovery-around-juniper-backdoor-raises-more-questions-about-the-company/ [https://archive.fo/ZesM4]

Over 80 U.S. software and hardware companies have close "partnership" relationships with the NSA.[68] For example, Microsoft's partnership relationship with the NSA (which precedes the VEP) provides the NSA knowledge of Microsoft software bugs before releasing them to the public or the anti-virus companies.[69] This means that, at regular intervals, the NSA is able to get access to all computers running Microsoft for a period of time before the holes in the code are patched. This sort of access has allowed the NSA to put Computer Network Extracting (CNE) keyloggers on between 50,000-100,000 computers.[70] A computer infected with a keylogger allows the NSA to read a record of *every key* typed, often in real time.

In 2013, the U.S. government stated that it would disclose all significant vulnerabilities discovered after 2010 on an ongoing basis.[71] Unfortunately, major breaches since that date show that promise has not been fulfilled. CIA cyber weapons revealed by WikiLeaks used undisclosed security vulnerabilities possessed by the CIA but concealed from manufactures like Apple and Google between 2013 and

---

68 Glenn Greenwald, *No Place to Hide*, pg 87-88 (Metropolitan Books 2014) accessible at https://static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf [https://archive.fo/wwV05]

69 Michael Riley, *U.S. Agencies Said to Swap Data With Thousands of Firms,* Bloomberg (6/14/2013), www.bloomberg.com/news/2013-06-14/us-agencies-said-to-swap-data-with-thousands-of-firms.html see also SPIEGEL Staff, *Prying Eyes Inside the NSA's War on Internet Security, DER SPIEGEL (December 28, 2014)* http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [https://archive.li/KzF31]

70 Floor Boon et al., *NSA infected 50,000 computer networks with malicious software,* NRC Media (November 23 2013), https://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487 [https://archive.fo/ilA9f] see also David E. Sanger and Thom Shanker, *N.S.A. Devises Radio Pathway Into Computers,* N.Y.TIMES (1/14/2014) https://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html [https://archive.fo/o4JJ4] see also Ryan Gallagher and Glenn Greenwald *How the NSA Plans to Infect 'Millions' of Computers with Malware,* The Intercept, (3/12/2014) https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware [https://archive.fo/DBHLh]

71 Richard A. Clarke et al., *Liberty and security in a changing world: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, The White House (12/12/2013), *accessible at* https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (last visited 2/25/2019)

2016.[72] In 2017, the United States' refusal to disclose such vulnerabilities under the VEP contributed to global cyberattacks tied to the Notpetya malware.[73] The Notpetya malware has caused nearly $10 billion in damage to businesses and organizations around the world. These financial losses continue to mount because much of the cyberattack is not covered by insurance policies.[74]

Again, there is a solution: attorneys should seek open-source products whose source code can be publicly accessed and vetted – to ensure there are no secret, government-prompted flaws that risk revealing client information.[75] Read more *infra* at The Duty to Use Open Source Software on Page 24.

## II. c. Parallel Construction

Information used daily in criminal proceedings across the U.S. is often gathered illegally, without the warrants or consent that would otherwise be required to

72 Symantec Security Response, *Longhorn: Tools used by cyberespionage group linked to Vault 7,* Symantec (4/10/2017) https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7 [https://archive.fo/59sSq] see also Wikileaks, *Vault 7: CIA Hacking Tools Revealed,* Wikileaks (3/7/2017) https://wikileaks.org/ciav7p1/ [https://archive.fo/3I3ps] see also Joe Uchill, *WikiLeaks' latest leak shows how CIA avoids antivirus programs,* The Hill (3/31/2017), http://thehill.com/policy/cybersecurity/326691-wikileaks-newest-cia-source-code-leak-shows-how-cia-avoids-anti-virus see also Sam Biddle, *The NSA Leak Is Real, Snowden Documents Confirm,* The Intercept (8/19/2016) https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/

73 Sam Biddle, *Leaked NSA Malware Threatens Windows Users Around the World,* The Intercept (4/14/2017) https://theintercept.com/2017/04/14/leaked-nsa-malware-threatens-windows-users-around-the-world/ see also Bryan Clark, *NSA knew about the vulnerability exploited by NotPetya for over 5 years*, The Next Web (6/27/2017) https://thenextweb.com/security/2017/06/27/nsa-knew-about-the-vulnerability-exploited-by-notpetya-for-over-5-years/ see also, Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History* Wired (9/2018) https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

74 Adam Satariano and Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.* The N.Y. Times, (4/15/2019) https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

75 The biggest difficulty in training professionals about mass surveillance and secure communications is that many professionals have assumed that it is too complicated for their organizations to use IT systems securely. Thankfully this is not true, and we have more tools at our disposal to secure information than ever before in human history. As Rob Feitel, a former career federal prosecutor at the Department of Justice stated "Only a foolish person understands your communications can be intercepted and does nothing about that…It's no different from locking your office door." (Quote from G. Alex Sinha, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy,* Human Rights Watch (07/28/2014)), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and# [https://archive.ph/pTluM]

initiate an intrusive investigation.[76] This is one of the most significant ways that clients' Fourth Amendment warrant requirements and Sixth Amendment right to counsel have been undermined in the surveillance age. Information gathered as part of the NSA's mass surveillance, is used as evidence by U.S. domestic police agencies in routine criminal cases. Through the use of a process called "parallel construction," the fact that such evidence originated from warrantless government spying is intentionally obscured from individuals and their attorneys.

Through electronic NSA mass surveillance of email, instant messaging, social media, text, and other communications, federal agents are able to search massive government databases for information on someone that they hope may relate to a crime. When something of interest is found they will send local police a "BOLO" (or "Be On the Look Out") order for the targeted person, with the specific instructions that local police must "[d]evelop your own probable cause for conducting a traffic stop."[77] When local police encounter the person they will then detain the person, looking for some evidence of a crime, evidence which was only originally discovered through warrantless information acquired by mass electronic surveillance. If local police find such evidence and initiate a criminal matter, they will then deny the origination of the evidence and cover the original electronic information with a false witness or confidential informant. Nancy Gertner, a Harvard Law School professor

76 Sarah St.Vincent, *The Dark Side: Secret Origins of Evidence in US Criminal Cases*, *pg 38*, Human Rights Watch (1/9/2018) https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases [https://archive.fo/Wjg5e]

77 BOLOs from intelligence contractor Stratfor: https://wikileaks.org/gifiles/docs/28/2870237_corrected-bolo-suspected-meth-smuggler-mexico-to-atlanta-ga-.html; https://wikileaks.org/gifiles/docs/28/2890348_fw-bolo-possible-narcotics-smuggling-.html;
https://wikileaks.org/gifiles/docs/29/2942193_fw-possible-narcotics-currency-trafficker-contact-sa-steven.html;
https://wikileaks.org/gifiles/docs/28/2833293_fw-bolo-narcotics-smuggling-white-denali-.html;
https://wikileaks.org/gifiles/attach/136/136917_BOLO-Possible%20Narcotics%20Smuggling.pdf;
https://wikileaks.org/gifiles/docs/28/2833019_bolo-possible-drug-smuggler-.html;
https://wikileaks.org/gifiles/attach/136/136844_2012-0086%20BOLO.pdf;
https://wikileaks.org/gifiles/docs/28/2886801_possible-alien-smuggling-in-ept-aor-.html; and
https://wikileaks.org/gifiles/docs/29/2943328_-alpha-insight-cbsa-2-aric-ag-3-cfix-ciac-2-and-dhs.html (all accessed 4/19/2019).

and former federal judge, in responding to the concept of parallel construction, said: "It sounds like they are phonying up investigations."[78]

This "phonying up investigations" is a routine practice of the U.S. Government. The Special Operations Division, a $125 million unit of the Drug Enforcement Administration (DEA), trains federal agents on parallel construction, and it is a formal policy to hide NSA data by covering it with false statements and fake witnesses.[79] Because nearly 94 percent of state-level felony convictions and 97 percent of federal convictions are the result of plea bargains, it is rare that defense attorneys have full access to the initiating evidence of many criminal cases.[80] In this way very few defendants ever suspect that the initiating evidence to start an investigation was obtained through illegal mass surveillance.[81] The use of this illegally acquired evidence in trials, often referred to "as the fruit of the poisonous tree" in evidentiary law, has therefore been hidden from attorneys, clients and the judiciary, threatening the integrity of the legal process.[82] This startling practice undermines the Sixth Amendment right of defendants to know the evidence that is being used

78 John Shiffman & Kristina Cooke, *U.S. directs agents to cover up program used to investigate Americans*, Reuters (8/5/2013), www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 [https://archive.fo/3OMgV]

79 John Shiffman & Kristina Cooke, *U.S. directs agents to cover up program used to investigate Americans*, Reuters (8/5/2013), www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 [https://archive.fo/3OMgV]

80 U.S. SENTENCING COMM'N, 2012 ANNUAL REPORT 42 (2012), available at (last visited 4/23/2019) http://www.ussc.gov/sites/default/files/pdf/research-and-publications/annual-reports-and-source-books/2012/2012_Annual_Report_Chap5.pdf. see also SEAN ROSENMERKEL ET AL., BUREAU OF JUSTICE STATISTICS, DEP'T OF JUSTICE, NCJ 226848, FELONY SENTENCES IN STAT E COURTS, 2006—STATISTICALTABLES 1 (2010), available at (last visited 4/23/2019) http://www.bjs.gov/content/pub/pdf/fssc06st.pdf see also Gaby Del Valle, *Most criminal cases end in plea bargains, not trials,* (8/7/2017) https://theoutline.com/post/2066/most-criminal-cases-end-in-plea-bargains-not-trials

81 Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, The Intercept (11/30/2017) https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/ SID Today, *The 'Dope' on the NSA-DEA Relationship*, The Intercept (9/13/2017), https://search.edwardsnowden.com/docs/TheDopeontheNSA-DEARelationship2017-09-13_nsadocs_snowden_doc [https://archive.fo/AL8M9]

82 Sarah St.Vincent, *The Dark Side: Secret Origins of Evidence in US Criminal Cases*, Human Rights Watch (January 9, 2018) https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases [https://archive.fo/Wjg5e] See also Trevor Aaronson, *Welcome to Law Enforcement's "Dark Side": Secret Evidence, Illegal Searches, and Dubious Traffic Stops,* The Intercept (1/9/2018) https://theintercept.com/2018/01/09/dark-side-fbi-dea-illegal-searches-secret-evidence/

against them in an open court, and it destroys an attorneys' ability to effectively serve their clients.[83]

Modern attorneys must be aware of this practice and do their best to represent criminal clients by finding out whether and how evidence against their client has been unconstitutionally collected. Fortunately, New York State has new criminal discovery laws that should empower attorneys to ask for, and receive, this kind of evidence before a plea bargain. For more information, see *infra* at The Ethical Duty of Zealous Representation and Digital Discovery on Page 26.

## III. Solutions: Modernizing Legal Ethics for the Digital Age

Knowing what we now know about government and corporate monitoring of many forms of online[84] and offline[85] communications, professional ethics fundamentally requires that lawyers protect privileged communication, because unless an attorney is properly securing privileged data, information harmful to a client could have come from their own attorney.[86]

83 Nicolas Niarchos, *Has the NSA Wiretapping Violated Attorney-Client Privilege?,* The Nation (2/4/2014), http://www.thenation.com/article/178225/has-nsa-wiretapping-violated-attorney-client-privilege [https://archive.fo/EdSzO]

84 Andrew Perlman, *Protecting Client Confidences in a Digital Age: The Case of the NSA,* JURIST Forum (March 4, 2014), http://jurist.org/forum/2014/03/andrew-perlman-client-confidences.php (last visited 2/25/2019) see also [http://archive.fo/sAF9c]

85 John Napier Tye, *Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans,* www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html see also Steven Melendez, *Suspicious packages spotlight vast postal surveillance system,* Fast Company (10.25.18), https://www.fastcompany.com/90257308/suspicious-packages-spotlight-vast-postal-surveillance-system-mail-covers [https://archive.ph/oxhC7] see also Julie Lynn Rooney, *Going Postal: Analyzing the Abuse of Mail Covers Under the Fourth Amendment*, Vanderbilt University Law School (2017) https://cdn.vanderbilt.edu/vu-wp0/wp-content/uploads/sites/278/2017/10/07094133/Going-Postal.pdf

86 Paul H. Beach, *Viewing Privilege Through a Prism: Attorney-Client Privilege in Light of Bulk Data Collection*, 90 Notre Dame L. Rev. 1663 (2014) available at https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4608&context=ndlr

A lawyer's duty of confidentiality is considered "the most sacred of all legally recognized privileges, and its preservation is essential to the just and orderly operation of our legal system."[87] The need to protect client confidentiality is specifically articulated in three distinct doctrines of law. The first is the lawyer's ethical duty of confidentiality,[88] second is the evidentiary privilege for attorney-client communications,[89] and third is the evidentiary privilege for attorney-client work-product.[90] These confidentiality obligations require that a lawyer's communication with clients or in pursuit of a client's case are private regardless of whether conducted on paper, in person, or electronically.[91] This duty includes avoiding the discussion of client matters in public locations, such as elevators, courthouse corridors, or on social media, where they could easily be overheard or shared.[92] Confidentiality is not simply a stand-alone duty of each attorney; it is also enforced by the rules of evidence, which bar admission of material protected by the attorney-client or work-product

87 *United States v. Bauer*, 132 F.3d 504, 510 (9th Cir. 1997).

88 The rules of professional conduct articulate the current ethical standards lawyers must uphold, stating "a lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." This confidentiality obligation has two aspects to it. It consists of both a prohibition and an affirmative duty. First, it prohibits the lawyer from disclosing confidential information about the client without client consent. Second the lawyer must not engage in casual or frivolous conversation about a client's matters that creates an unreasonable risk of harm to the interests of the client.

89 The rules of evidence are designed to enforce confidentiality in the context of adversarial proceeding. They provide a near absolute bar on discovery of confidential attorney-client communications concerning the seeking or providing of legal advice. The lawyer must ensure that only the lawyer and the client are privy to such communications in order to properly invoke the evidentiary privilege. Lawyers are required to refuse to testify in court concerning any evidence that might be detrimental to a client. They must argue that their refusal is consistent with the privilege and, if the lawyer is subject to an adverse decision on the issue, to seek a possible appellate review, including suffering a contempt citation to force a further adjudication of the privilege claim.

90 Evidentiary law also protects the confidentiality of client information using the attorney work product privilege. This legal doctrine applies to work undertaken by all parties under the direction and control of the attorney in anticipation of or during actual litigation. The privilege prevents inquiry into any activities lawyers must do in order to provide competent legal services. This includes but is not limited to, research, witness and consultant interviews, conversations reviewing documents, engagements with expert witnesses, and most other tasks required by an attorney in the course of providing effective representation.

91 *Upjohn Co. v. United States*, 449 U.S. 383, 389, 101 S.Ct. 677, 682, 66 L.Ed.2d 584 (1981).

92 See In re Victor, 422 F. Supp. 475, 476 (S.D.N.Y. 1976) (finding no privilege for documents placed in a public hallway since "it certainly could not be said that the client expected these papers to be kept from the eyes of third parties.") See also, e.g., Suburban Sew'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254 (N.D.Ill. 1981); Schwartz v. Wenger, 124 N.W.2d 489 (Minn. 1963) (testimony of nonsurreptitious eavesdropper who overheard client-lawyer conversation in crowded courthouse hallway admissible because no effort made by client or lawyer to ensure secrecy).

privilege.[93] However, in order for lawyers to invoke an evidentiary bar, the rules of evidence require that lawyers resist, to the extent legally permissible, any attempt by others to access privileged information.[94] This important ethical principal is articulated in Rule 1.6 of the Model Rules which state, "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[95]

---

93 The federal rules of evidence define this requirement utilizing eight factors: the communication must be (1) legal advice sought from a (2) professional legal advisor (3) where the communication is related to the legal purpose, and (4) is made in confidence, (5) by the client, and (6) is permanently protected for the client (7) from disclosure by himself or the legal advisor, (8) unless that protection is waived. (FED. R. EVID. 501. 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2292, at 554 (McNaughton rev. 4th ed.1961)).

94 Model Rules of Prof'l Conduct R. 1.6, (2005); State v. Schubert, 235 N.J. Super. 212 (App. Div. 1989). See also, Restatement (Third) of the Law Governing Lawyers § 60 (2000).

95 Model Rules of Prof'l Conduct R. 1.6, (2005) As the comments to 1.6 read, the, "fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation." (cmt. 13) In 2012 the American Bar Association (ABA) modified the language of the applicable rule to impose an explicit obligation on attorneys to take positive steps to protect the confidentiality of information concerning their clients and cases. (American Bar Association (ABA), Amendments to Model Rules of Professional Conduct,(8/2012) available at https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_house_action_compilation_redline_105a-f.authcheckdam.pdf, pp. 5-7 (last visited 2/25/2019))._ The ABA rule has a "reasonableness test"; and the commentary elaborating it identifies several factors that lawyers must weigh in discerning the measures they are reasonably expected to undertake to protect their communications. Those factors include (but are not limited to): the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). The ABA also released Ethics Opinion 477 (5/11/2017) on encryption of attorney-client communication stating that "Model Rule 1.4 may require a lawyer to discuss security safeguards with clients" and that "a fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances". (ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477 (2017)) Each State bar has its own interpretation of how to define "reasonable effort." Pennsylvania's State bar, for example, has defined reasonable effort in a way that specifically encourages attorneys to regularly use encryption to protect their clients. The Professional Ethics Committee for the State Bar of Texas found many common situations where a lawyer would be "prudent to use encrypted email." (The Professional Ethics Committee for the State Bar of Texas, Opinion No. 648 (2015) *available at* https://www.law.uh.edu/libraries/ethics/opinions/601-700/EO648.pdf) Ultimately clients control attorney client privilege because, according to Rule 1.2 of Model Rules of Professional Conduct (2018), "a lawyer shall abide by a client's decisions concerning the objectives of representation and…shall consult with the client as to the means by which they are to be pursued." This rule makes it clear that clients control attorney client privilege and can instruct attorneys to uniformly apply security measures, including encryption to all attorney client communications.

While attorney client privilege is recognized in legal systems around the world, the right to privacy, as defined in international law also provides a consistent global standardizing framework for attorney-client communications.[96]

### III. a. The Duty to Encrypt

The most robust technical way of protecting attorney-client communications in the 21st century is the uniform use of end-to-end encryption. Encryption is – simply – writing in code. Current encryption programs apply very rigorous math, logic, and technology to the basic process that all people engage in when creating dialects or languages.[97] In an interesting twist of technological progress, the current application of this science allows for anyone with a home computer to create encryption advanced enough that, when properly implemented, it cannot be broken by all

96 The right to privacy is articulated in its most expansive form in the Universal Declaration of Human Rights, Article 12, which states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence." (UN General Assembly. (1948). Universal declaration of human rights (Article 12)). The International Covenant on Civil and Political Rights (ICCPR) Article 17 (12/16/1966) contains the articulation of these aspirational human rights in an enforceable treaty. Article 17 of the ICCPR states "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.." (International Covenant on Civil and Political Rights (ICCPR) Article 17, United Nations Treaty Series at 999 U.N.T.S. 171 (12/16/1966)). As of April 2018, the ICCPR has been ratified by 170 state parties and is monitored by the United Nations Human Rights Committee. The U.S. formally ratified the ICCPR on June 8, 1992. Upon US ratification of ICCPR, the U.S. has the legal obligation to implement the treaty and report to the United Nations (UN). Under the Supremacy Clause of Article VI of the U.S. Constitution, the treaty became the binding law in the United States as any other federal law would be, and preempts all state laws.(U.S. Const. art. VI) The majority of legal licensing systems have similar human rights and ethics based confidentiality requirements for attorney-client privileged material. Since at least 2015 the UN has begun including robust attorney-client privilege ethical protections into its framework for investigating human rights abuses and for human rights attorneys.

97 Help Net Security, *Encryption use continues to grow*, (2/11/2014) http://www.net-security.org/secworld.php?id=16340 see also Klint Finley, *Encrypted Web Traffic More Than Doubles After NSA Revelations,* Wired (5/16/2014) https://www.wired.com/2014/05/sandvine-report/ [https://archive.fo/aAy08]

the computer power in the world.[98] End-to-end encryption means *only* the communicating users can read the messages they send to each other.[99] Many encryption programs have been released that cost the user nothing and can save organizations and business significant amounts when integrated into cybersecurity planning. [100]

The technological tools to resist mass surveillance and protect attorney-client privilege are inexpensive, usable and ubiquitous.[101] But these tools will never gain the broad reach they need to be effective unless attorneys and civil society organizations are educated and empowered to adopt their use. Secure communications cannot be established on an individual basis, since all parties engaged in communications must adopt secure practices. Secure communications are therefore necessarily a network-based and profession-wide practice.

Attorneys are far behind their counterparts in other professions and practice areas in taking the risks of digital surveillance seriously. Members of professions with less rigorous ethical and regulatory requirements are now practicing more robust security than most attorneys. Many states' consumer regulations are also

---

98 Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* John Wiley & Sons, Inc. (1993) https://archive.org/details/AppliedCryptographyBruceSchneier

99 End-to-end encryption prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt a conversation. As Snowden has stated, "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on." This means that an everyday computer user with medium competency can currently download a free open source encryption program from the Internet that, when properly implemented and verified, allows them to encode information in a way that is impossible for even the largest actors, like the NSA to break.

100 SPIEGEL Staff, *Prying Eyes Inside the NSA's War on Internet Security,* DER SPIEGEL (12/28/2014) https://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [https://archive.fo/KzF31] see also Bruce Schneier, *Attacking Tor: how the NSA targets users' online anonymity,* The Guardian (10/4/2013), www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity [https://archive.ph/gpShR] Brian Barrett, *Don't Let WikiLeaks Scare You Off of Signal and Other Encrypted Chat Apps* https://www.wired.com/2017/03/wikileaks-cia-hack-signal-encrypted-chat-apps/ Wired (3/7/2017) see also Sam Biddle & Micah Lee, *The CIA Didn't Break Signal or WhatsApp, Despite What You've Heard* https://theintercept.com/2017/03/07/the-cia-didnt-break-signal-or-whatsapp-despite-what-youve-heard/ The Intercept (3/7/2017)

101 Electronic Frontier Foundation, *Surveillance Self-Defense*, https://ssd.eff.org/en/index

ahead of attorneys in specifying the types of security needed for business relationships. Nevada, New York[102] and Massachusetts have legally mandated encryption requirements as part of their consumer protection regulations.[103] The Massachusetts Attorney General has been active in enforcing this part of its state's consumer data protection regulations against entities that have lost unencrypted client data.[104]

In New York, the New York State Department of Financial Services has put new regulations governing cybersecurity fully into effect in 2020. [105] The regulations recognize that because "cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data... certain regulatory minimum standards are warranted." The NYSDFS regulations require "Covered Entities" to establish and maintain a comprehensive cybersecurity programs, which can include law firms or lawyers that are working under "Banking Law, the Insurance Law or the Financial Services Law." These organizations are required, among other

102 In New York, beginning in March 2017, the Department of Financial Services ("NYDFS") promulgated regulations that broadly regulate cybersecurity within the financial services industry. NYDFS is the New York state regulator of financial services licensed in the state and thus supervises many large banks and insurance companies, including law firms that work with them. (NY State Dept. of Fin. Ser. *Cybersecurity requirements for financial services companies* 23 NYCRR 500 (3/1/2017) available at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf)

103 Massachusetts information security law, M.G.L. c. 93H, applies to "persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." The law applies to all private businesses including lawyers and law firms and requires that an organization have a written security plan that includes "to the extent technically feasible, . . . encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly." See also MA General Laws, Chapter 93H: https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H. Nevada gives the Payment Card Industry Data Security Standard ("PCIDSS"), an industry standard developed by a private rule-making body, the force of law in the state. The PCIDSS aspect of the law requires all data collectors who do business in the state of Nevada and that accept a payment card in connection with a sale of goods or services must maintain their personal data securely. The second set of provisions requires encryption of personal information during electronic transmission or while in storage on data storage devices..

104 This enforcement against an out-of-state businesses having sufficient minimum contacts with the Commonwealth of Massachusetts demonstrates that the Massachusetts Attorney General has been aggressively engaged in enforcing both Federal and Massachusetts information security law against all entities who do not use robust encryption to store the personal data of Massachusetts residents and may be a model for enforcement by other states.

105 NY State Dept. of Fin. Ser. *Cybersecurity requirements for financial services companies* 23 NYCRR 500 (3/1/2017) available at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

things, to perform a risk assessment of their cyber risks, implement a written cybersecurity policy, and maintain a comprehensive cybersecurity program which "shall implement controls, including encryption, to protect Nonpublic Information."[106]

It is also illuminating to compare the practice of the Bar to the ethics of journalists. Both professions have similar professional obligations to provide confidentiality to clients and sources.[107] By 2019 most major print media, from the New York Times to USA Today to The Intercept offer open source encrypted drop boxes for first contact with sources and more than two-thirds of journalists and newsrooms use end-to-end encryption tools -- nearly a 50% increase since 2017.[108] This is an area where the legal profession must learn from the practice of other professionals like journalists, and enforce encryption for first contact with new clients. For example, websites for major New York whistleblower law firms must install technically confidential and anonymous drop-boxes for information submission and first contact with whistleblowers; unfortunately, this is far from current industry practice.[109]

Of course, attorneys often engage with consumer financial transactions, health data, and appeals to whistleblowers. Complying with cybersecurity rules is becoming a mandate driven by compliance with piecemeal regulations, developed in specific subject-matter areas by legislators and regulators outside of the legal profession. This results in a two-tiered system of justice, where only legal clients whose work or identity falls into specifically regulated areas receive the gold standard of

---

106 NY State Dept. of Fin. Ser. *Cybersecurity requirements for financial services companies* 23 NYCRR 500 (3/1/2017) available at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

107 When looking at the global media landscape in the period from 2006-2010 the only major media outlet that provided robust digital security to sources was Wikileaks. Only after the Snowden revelations of US government mass surveillance in 2013, did thousands of individual journalists began to adopt open source encryption tools to provide sources with secure mean of first contact and follow up. See also Dave Segalin, *The Case for Encryption*, Canadian Journalist for Free Expression (2015) https://www.cjfe.org/the_case_for_encryption

108 International Center For Journalists, *The State of Technology in Global Newsroom,* ICFJ (2019), https://www.icfj.org/sites/default/files/2019-10/2019%20Final%20Report.pdf see also SecureDrop https://securedrop.org/directory/

109 Some illustrative examples of whistleblower law firms without any means of anonymous first contact with clients: Phillips & Cohen: https://www.phillipsandcohen.com/ Also, Kohn, Kohn & Colapinto LLC: https://www.kkc.com/should-i-be-an-anonymous-and-confidential-whistleblower/ Also Hagens Berman LLP: https://www.hbsslaw.com/about-us/tip-line Only the firm "Whistleblower Aid" seems to have a fully technically anonymous contact system: https://whistlebloweraid.org/contact/#whistleblower-contact

cybersecurity. Such regulations are deeply inequitable – and undoubtedly result in the best and most confidential representation going only to the most monied financial clients. It is also an indictment of the legal profession and its regulatory bodies: other professions recognize that digital threats require technical safeguards for client transactions. The bar must follow suit. Here are recommendations that will change individual attorney and bar association practice:

- Attorneys must change ethical standards to require that all members of the profession use end-to-end open source encryption for privileged attorney-client communications. One of the highest traditions of an independent bar is the inherent power to establish standards for lawyer conduct and to ensure lawyers can meet those standards.[110] To properly secure attorney-client information, Electronic Frontier Foundation's Surveillance Self-Defense[111] guide is a good resource to get started securing your privileged communications. Also the Alternative App Centre and Security in a Box, by Tactical Technology Collective and Front Line Defenders [112] have many end-to-end open source tools[113] that attorneys can use to immediately begin to encrypt their Attorney Client communications.
- The ABA, state level bar associations, state financial control boards, offices of privacy, and offices of consumer regulations must adopt regulatory standards

110 See, e.g., *Upjohn Co. v. United States*, 449 U.S. 383, 389, 101 S.Ct. 677, 682, 66 L.Ed.2d 584 (1981); ("[t]he privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client."); *Fisher v. United States*, 425 U.S. 391, 403, 96 S.Ct. 1569, 1577, 48 L.Ed.2d 39 (1976) ("[t]he purpose of the privilege is to encourage clients to make full disclosure to their attorneys... it protects only those disclosures, necessary to obtain informed legal advice, which might not have been made absent the privilege"). In re Vanderbilt (Rosner-Hickey), 439 N.E.2d 378, 384 (N.Y.1982) ("[t]he privilege is intended to foster openness between counsel and client so that legal problems can be thoroughly and accurately analyzed").

111 Electronic Frontier Foundation, *Surveillance Self-Defense*, https://ssd.eff.org/en/index

112 Alternative App Centre: https://myshadow.org/resources, Tactical Technology Collective and Security In a Box https://securityinabox.org/en/about/ by Front Line Defenders and Tactical Technology Collective,

113 For example, Moxie Marlinspike, *Signal Messenger 2013-2018,* https://github.com/signalapp See also https://signal.org/ See also Signal Foundation https://signalfoundation.org/ See also Proton Technologies AG, https://protonmail.com/ see also https://github.com/ProtonMail See also Wire, https://wire.com/en/download/ See also Secure Drop https://securedrop.org/ See also The Matrix.org Foundation C.I.C. (2019) https://github.com/matrix-org

that enforce open source end-to-end encrypted technology for all attorney-client privileged communications.

- Attorneys, clients, and professional associations should advocate for federal level regulation or legislation to incorporate standards requiring open source end-to-end encrypted communications for all attorney-client communications.
- Attorneys, clients, and professional associations should advocate within the UN Human Rights bodies and the ethics bodies of the International Criminal Court (ICC) to require encrypted communications for global attorney-client communications.
- New York State Department of Financial Services regulations should be expanded to include requiring end-to-end encryption for all attorney-client communications with New York State residents as a whole.[114]

### III. b. The Duty to Use Open Source Software

Proprietary software products, like Microsoft and Apple Operating Systems, all create legal and technical prohibitions on users and engineers that keep them from viewing the actual functioning of the source code that makes computer programs run. Proprietary software, also referred to as "closed source" or "non-free" software, includes copyright terms that give intellectual rights to the source code to someone other than the user. These exclusive rights over the software allow the owner to restrict use, inspection of source code, modification of source code, and redistribution. As demonstrated in the discussion of the VEP *supra*, this lack of user rights to software has negative real world impacts on the security of these software systems.

The solution is for attorneys to seek out open source software that allows for a more scientific process of transparent and verifiable software improvements that

114 NY State Dept. of Fin. Ser. *Cybersecurity requirements for financial services companies* 23 NYCRR 500 (3/1/2017) available at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

are not dependent on a closed group that could be directly cooperating with a government intelligence service, like the NSA.[115] Open source software, like Ubuntu or Debian, allows for software engineers and users to fully control all aspects of a computer system. [116] Detailed studies have proven that specific open source operating systems like Linux are more bug free then proprietary systems.[117] This allows engineers and users to quickly and effectively fix their computer if it has been compromised.[118] It is a great benefit that open source programs are generally free of cost to the users. Many countries, including the governments of the US, Uruguay, Ecuador, and Brazil are now running some or most of their information technology on open source platforms.[119] Here are recommendations that will change individual attorney practice and bar association guidelines:

- Attorneys should inform themselves about open source platforms and use them whenever possible. A good resource for Free Software and Open

115 SPIEGEL Staff, *Prying Eyes Inside the NSA's War on Internet Security, DER SPIEGEL (December 28, 2014)*http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html [https://archive.fo/KzF31] see also Bruce Schneier, *Attacking Tor: how the NSA targets users' online anonymity,* The Guardian (4 October 2013 15.50 BST), www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity [https://archive.ph/gpShR]

116 Micah Lee, *Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance*, Freedom of the Press Foundation, (last visited 2/26/2019) https://github.com/freedomofpress/encryption-works/blob/master/encryption_works.md [https://archive.fo/QobXQ] see also Trevor Timm, *Help Support the Little-Known Privacy Tool That Has Been Critical to Journalists Reporting on the NSA*, Freedom of the Press Foundation (4/2014), https://freedom.press/news-advocacy/help-support-the-little-known-privacy-tool-that-has-been-critical-to-journalists-reporting-on-the-nsa/ [https://archive.fo/REujS]

117 A study found Linux containing 985 bugs in 5.7 million lines of code, while the industry average for commercial enterprise software has 20 to 30 bugs for every 1,000 lines of code. WIRED Staff, *Linux: Fewer Bugs Than Rivals,* Wired (12/14/2004), https://www.wired.com/2004/12/linux-fewer-bugs-than-rivals/ [https://archive.ph/Qfxs5] see also DOD CIO *Clarifying Guidance Regarding Open Source Software (OSS)*. 10/16/2009 http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf

118 Auguste Kerckhoffs "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883. See also *Bellovin, Steven; Bush, Randy,* Security Through Obscurity Considered Dangerous, Internet Engineering Task Force (IETF), (2/2002) https://www.cs.columbia.edu/~smb/papers/draft-ymbk-obscurity-00.txt

119 "Software Libre en América Latina" www.telesurtv.net/news/Software-Libre-en-America-Latina-20140919-0071.html [https://archive.fo/gGmAw] see also *The adoption of free and open-source software by public institutions, Wikipedia,* https://en.wikipedia.org/wiki/Adoption_of_free_and_open-source_software_by_public_institutions (last viewed 2/26/2019) [https://archive.fo/ANER3] See also Tony Scott, *Federal Source Code Policy*, Office of Mgmt. & Budget, Exec. Office of the President, 9/8/2016 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_21.pdf

Source[120] privacy protecting software is Privacy Tools[121] or the Alternative App Centre, and Security in a Box, by Tactical Technology Collective and Front Line Defenders.

- Attorneys, clients, and professional associations should advocate that open source privacy focused operating systems are utilized for all attorney-client drafting and at rest encryption.[122]

- Professional legal associations should offer services to assist civil society organizations and legal services offices to achieve security audits and internal reviews to assess the security of their privileged communications.
- Professional legal associations should offer trainings to organizations to educate them about how to utilize open source end-to-end encryption whenever they have clients who need the services of an attorney.

### III. c. The Ethical Duty of Zealous Representation and Digital Discovery

In addition to the duty of confidentiality, attorneys "zealously asserts the client's position."[123] When it comes to criminal representation, attorneys have an ethical duty to make every effort to determine if their clients evidentiary, due process, Fourth,[124] Fifth,[125] or Sixth Amendment rights have been violated.[126]

120 Free Software Foundation: https://www.fsf.org/
121 Privacy Tools: https://PrivacyTools.io
122 For Example, Tails Operating System: https://tails.boum.org/ or Qubes OS https://www.qubes-os.org/
123 Model Rules of Professional Conduct: Preamble, Section 2 https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_preamble_scope/
124 Fourth Amendment, The Legal Information Institute at Cornell Law School https://www.law.cornell.edu/constitution/fourth_amendment
125 Fifth Amendment, The Legal Information Institute at Cornell Law School https://www.law.cornell.edu/constitution/fifth_amendment
126 Sixth Amendment, The Legal Information Institute at Cornell Law School, https://www.law.cornell.edu/constitution/sixth_amendment

Given the widespread use of electronic surveillance and the existence of parallel construction, *see supra,* zealous representation in any criminal case should include an attorney's efforts to sniff out unlawful or warrantless surveillance that might have served as a source for evidence collected against a client. In *Carpenter v. United States*,[127] the United States Supreme Court held that digital location data is protected by the Fourth Amendment and cannot be obtained by police without a warrant, even where that data is provided by a private company. *Carpenter* is the latest in a line of cases suggesting that the Supreme Court is willing to apply more robust warrant requirements and privacy rights to criminal cases. The legal profession needs criminal discovery rules that reflect this outlook.

Discovery reforms passed by New York State in 2019 are an important first step to remedying New York's antiquated discovery rules. [128] The new discovery rules specify twenty one different kinds of materials that prosecutors must turn over to the defense. This includes many items were not previously listed[129] such as "all tapes or other electronic recordings,"[130] and "a copy of all electronically created or stored information seized or obtained by or on behalf of law enforcement."[131] They also require the prosecution turn over "all evidence and information...that tends to: (i) negate the defendant's guilt as to a charged offense,"[132] so called "Brady Material," which is information favorably related to the innocence of the accused.[133]

The new open file discovery rules should require that law enforcement turn over all case information except information which could directly harm human life, such

127 Carpenter v. United States, No. 16-402, 585 U.S. ____ (2018)
128 Governor Cuomo Announces Highlights of FY 2020 Budget (4/1/19) https://www.governor.ny.gov/news/governor-cuomo-announces-highlights-fy-2020-budget
129 Krystal Rodriguez, *Discovery Reform in New York: Major Legislative Provisions,* Center for Court Innovation (5/19) https://www.courtinnovation.org/sites/default/files/media/document/2019/Discovery-NYS_Full.pdf
130 The Laws of New York Consolidated Laws Criminal Procedure Part 2: The Principal Proceedings Title J: Prosecution of Indictments In Superior Courts--plea to Sentence: Section C.P.L. § 245.20(1)(g) https://www.nysenate.gov/legislation/laws/CPL/A245 see also C.P.L. § 245.20(1)(a)-(u).
131 Section C.P.L. § 245.20(1)(u)(i) https://www.nysenate.gov/legislation/laws/CPL/245.20
132 Section C.P.L. § 245.20(1)(k)(i) https://www.nysenate.gov/legislation/laws/CPL/245.20
133 Brady v. Maryland, 373 U.S. 83at 87(1963)

as the identity of confidential informants. However, the positive changes to the discovery rules are still unclear to the extent that they require the police to uncover new or supposedly "classified" technology as part of a request. Disclosing the technology, means, or methods would not harm any person. Without this level of disclosure discovery reform will not address the grievous harm done to the criminal process by the use of electronic mass surveillance and parallel construction. We believe there should be a definitive ruling or legislative change not only in favor of revealing sources of the information but also in revealing the technology and methods for acquiring that information.[134]

New York must expand its discovery reforms so that defense attorneys will know exactly which methods and with what technology surveillance is being conducted. Here are recommendations that will change individual attorney and bar association practice:

- Defense attorneys must craft discovery requests with an awareness of the possibility of parallel construction and attempt to use different strategies to find such illegal evidence. A careful eye towards cases that are suddenly dropped or charges that are vastly reduced after specific attorney evidence requests about overbroad surveillance can reveal the presence of illegally acquired evidence and methods in a case.[135] Patterns of unexplained dropped charges can reveal confidentiality agreements with agencies that may utilize parallel construction. For example, through a FOIL records request the NYCLU was able to prove that FBI Nondisclosure agreements[136] instruct the

134 Legislative Memo: Discovery Reform(2019) https://www.nyclu.org/en/legislation/legislative-memo-discovery-reform see also Senate Bill S1716 (2019-2020 Legislative Session) https://legislation.nysenate.gov/pdf/bills/2019/S1716

135 NYCLU "Erie County Sheriff Records Reveal Invasive Use of "Stingray" Technology" (4/7/2015)*Available at*: https://www.nyclu.org/en/press-releases/erie-county-sheriff-recordsreveal-invasive-use-stingray-technology.

136 NYCLU "RPD's Non-Disclosure Agreement" https://www.nyclu.org/sites/default/files/2012_HarrisCorp_NDA%282016-03-11_pgs135-141%29.pdf

Rochester County Sheriff's Office to dismiss criminal prosecutions rather than risk compromising the secrecy of surveillance technology it is using.

- Achieve more transparency of government snooping methods, as well as disclosure of all evidence collected or held by the government which is favorable to the defense.

- For services that lack clear replacements, like legal search software vendors Lexis and Westlaw, attorneys need full transparency to ensure their search results are not manipulated or monitored to negatively impact clients' interests. Any ethical search provider must provide robust open source transparency on search algorithms and options for anonymous searching of their legal data basis for unmonitored attorney research. Attorneys and their professional associations should advocate with legal research companies for such transparency and privacy guarantees as a core aspect of their services.