Why Attorneys Must Encrypt Privileged Communications with Clients

> "We need new professional training and new professional standards to make sure that we have mechanisms to ensure that the average member of our society can have a reasonable measure of faith in the skills of all the members of these professions." - Edward Snowden

There are many digital threats that can undermine the security of attorney-client communications, from private hackers to surveillance by multiple government agencies. One of the most serious threats is the use of evidence that has been gathered through NSA mass surveillance by domestic police agencies in criminal investigations. This information is gathered illegally, without the warrants that would otherwise be required to initiate an investigation. Through the Special Operations Division, a $125 million unit of the Drug Enforcement Administration (DEA), **Police officers are trained to utilize a process called "parallel construction" to hide NSA data by covering it with fake witnesses**. The use of this illegally acquired evidence in trials has therefore been hidden from attorneys, clients and the judiciary, threatening the integrity of the legal process. This startling practice undermines the Sixth Amendment right of defendants to know the evidence that is being used against them in an open court, and it destroys an attorneys' ability to effectively serve their clients.

The current vice chairman of the criminal justice section of the American Bar Association, James Felman, calls this domestic use of NSA intercepts "outrageous" and "indefensible." Nancy Gertner, a Harvard Law School professor and former federal judge, said that, **"It sounds like they are phonying up investigations."** Under its NSA Mass Surveillance programs, the US Government has taken privileged information from US attorneys. For example, the NSA illegally obtained information from Mayer Brown, a major Chicago based law firm involved in trade negotiations, and used it against them in those negotiations. Prosecutors have begun investigation of clients based on this illegal electronic dragnet information. In this way, prosecutors can even use privileged information between defense attorneys and clients in court against a defendant. Currently it is unclear how many thousands of cases may be based on this type of illegal evidence.

Professional Ethics fundamentally requires that lawyers protect privileged attorney-client communication. Knowing what we now know about government monitoring of many forms of online communications, **attorneys must update their ethical requirements to require encryption for all attorney client communications.** Unless an attorney is properly securing privileged data evidence against a client could have come from an attorney. To properly secure attorney-client information 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.

What you can do: Sign the petition to attorney organizations to update ethical rules to require the provision of end-to-end open source encryption for attorney client communication.