Published on *The National Law Review* https://natlawreview.com

Setting the Record Straight on the Legal Protections for the Ukraine Whistleblower: “No One Volunteers for the Role of Social Pariah”

Article By:

Stephen M. Kohn

Ever since news broke that a whistleblower had filed the “urgent concern” alleging misconduct in a phone call between President Donald Trump and Ukraine’s President Volodymyr Zelensky controversy has surrounded the rights of the whistleblower and whether his or her identity should be confidential. This debate has intensified after President Trump retweeted an article that identified the whistleblower by name. As an attorney who successfully sued the Clinton administration regarding the privacy rights of employees who accused President Clinton of impeachable offenses would like to clarify certain issues.

There are specific laws that apply to the Ukraine whistleblower, and they need to be understood by every Member of Congress who will vote on impeachment and every American voter who will be asked to decide whether President Trump should be re-elected.

Right to Privacy

Any analysis regarding the rights of the Ukraine whistleblower must start with a review of the actual six-page Disclosure Form the whistleblower filled-out when making the report concerning the Trump-Zelensky call. When filing the initial allegation the intelligence community a whistleblower had to fill out a detailed Form entitled “Disclosure of Urgent Concern Form.” That Form was thereafter filed with the Intelligence Community Office of Inspector General (“ICIG”).

The Disclosure Form provides intelligence community employees with two assurances that their confidentiality will be protected. First, the Form states that the information provided by whistleblowers is covered under the Privacy Act. The Privacy Act of 1974, 5 U.S.C. § 552a was passed after the Nixon White House was caught trying to obtain embarrassing information about another whistleblower, Daniel Ellsberg, in an attempt to discredit him. The Privacy Act is very comprehensive and contains both criminal and civil penalties.

Second, the Disclosure Form contains the following statement at the signature block where the whistleblower had to sign the form: “*I understand that in handling my disclosure, the ICIG shall not disclose my identity without my consent, unless the ICIG determines that such disclosure is*

unavoidable during the course of the investigation or the disclosure is made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken."

That statement reflects the rules on confidentiality governing the Intelligence Community Inspector General. The Inspector General Act mandates confidentiality for whistleblowers.

Thus, it cannot be reasonably contested that the original disclosure by the whistleblower to the OIG was confidential, and the whistleblower's identity was fully protected under two separate laws and pursuant to the written agreement signed by the employee when making the actual disclosure. The policy reasons behind this procedure serve the public interest. In exchange for the intelligence community legally and responsibility making disclosures to an Inspector General, the government agrees to keep the identity of the whistleblower confidential. This is an appropriate and lawful *quid pro quo*.

Review by the DNI

Once the whistleblower filed the "urgent concern" complaint, the Intelligence Community Inspector General was required to investigate the allegation and make a determination, within 14 days, as to whether or not the concern was "credible." If credible, the Inspector General was required to submit the whistleblower's information and a report to the Director of National Intelligence (DNI). The DNI was thereafter required to submit the allegation to the intelligence committees of Congress within seven days. These procedures are spelled out in the law, and there are no exceptions.

The "urgent concerns" disclosure rules determine precisely who can obtain lawful access to the whistleblower's identity and a copy of the original complaint. This type of procedure is required under the Privacy Act, as it spells out the rules governing access to sensitive information, and explains which offices of the federal government can learn the identity of a highly confidential source. Also, in accordance with the Privacy Act, all of the offices permitted to have access to the whistleblower's name, i.e. the Inspector General and the DNI, have a legal duty to shield the whistleblower's name from unauthorized disclosure.

The law does not permit the DNI to submit the whistleblower's identifying information to the White House. If such a disclosure happened, the DNI violated the Privacy Act. Additionally, the law covering "urgent disclosures" does not authorize the DNI to submit identifying information regarding the whistleblower to the Attorney General. Such a disclosure could also violate the Privacy Act.

This leaves a question that needs to be answered. How did anyone in the news media or the White House discover who the whistleblower is if the agencies of the federal government that had lawful access to the whistleblower's information were required, as a matter of law, to protect the whistleblower's identity?

The Intelligence Community Whistleblower Protection Act ("ICWPA")

Based on the public record it appears as if the Privacy Act has been violated and the confidentiality protections afforded to the Ukraine whistleblower under the Inspector General Act were not followed. Assuming this is the case, how can the whistleblower's rights under federal law be vindicated? The answer rests with the rights afforded the Ukraine whistleblower under the Intelligence Community Whistleblower Protection Act ("ICWPA"). This law prohibits retaliation against any intelligence community employee who makes a disclosure regarding "urgent concerns" to the Office of Inspector General, including allegations of an "abuse of authority" within the White

House. The Ukraine whistleblower is clearly covered under the ICWPA and retaliation against him or her is illegal.

The next question is widely disputed: Is a violation of confidentiality an adverse action under the ICWPA? Supporters of President Trump have argued that this law only protects whistleblowers from concrete employment actions, such as a termination or demotion. They claim that guarding a confidential informant's identity is not prohibited under the ICWPA, and the blowing a whistleblower's cover is not an adverse action.

Years ago the U.S. Supreme Court ruled that anti-retaliation laws are not limited only to correcting "concrete" employment actions, like a discharge. Instead, these laws cover a host of adverse actions that could "dissuade a reasonable employee" from making a protected disclosure. If CIA or intelligence community employees feared that the privacy protections afforded under the law would not be applied to them, would that cause a chilling effect on their willingness to blow the whistle? That question has been answered many times. But even if there were no cases on-point, the disclosure of a CIA employee's identity would severely limit, if not destroy, their employment prospects with that highly secretive agency.

Directly on point, in the *Haliburton v. Administrative Review Board case* in which the U.S. Court of Appeals for the Fifth Circuit awarded a whistleblower over $30,000 in damages based solely on a company's failure to keep his identity secret. The Haliburton *court* explained that the case hinged on the issue of whether "Halliburton's disclosure of [the whistleblower's] identity was a "materially adverse" action. The Court reasoned: "The undesirable consequences" of outing a whistleblower were "obvious." "In a workplace environment" "where collaboration is an important part of the job" the "targeted disclosure" of a whistleblower's identity would reasonably create "an environment of ostracism" and "dissuade a reasonable employee from whistleblowing." Or to put it more bluntly, "no one volunteers for the role of social pariah."

Although leaking a whistleblower's name is a violation of the ICWPA, there remains another major problem. The ICWPA is unlike any other whistleblower protection law. It does not vest enforcement authority with the courts or an independent administrative agency (like the Department of Labor). Instead, given the extreme importance of ensuring that intelligence community whistleblowers who raise "urgent concerns" are fully and completely protected, *the law vests the enforcement authority directly with the President of the United States.* The Intelligence Community Whistleblower Protection Act could not be clearer: **"[t]he President shall provide for the enforcement of the [Act].**" President Trump is mandated by law to protect the Ukraine whistleblower, ensure that he or she suffers no retaliation, and enforce the rules on confidentiality. This is a non-discretionary duty.

It is as simple as that. The President "shall" "enforce" the whistleblower law that makes it illegal to retaliate against the Ukraine whistleblower or to expose his or her identity. Unfortunately, as demonstrated by his public comments and Tweets, it is the President himself who is engaging in the retaliation. This is a unique circumstance in American legal history. It would be the equivalent of a judge in a sexual harassment case stepping off the bench and commencing to sexually harass the victim seeking protection in his courtroom. Perhaps there is some precedent for this in the old segregated South, when the state judges participated in discrimination, but in the history of federal whistleblower laws, it is simply unprecedented.

Obstruction of Justice

Finally, the Ukraine whistleblower is also protected under the obstruction of justice laws. The obstruction laws kick-in when a whistleblower decides to make his or her disclosure to a federal law enforcement agency, such as an Inspector General. In the case of the Ukraine whistleblower's disclosure was made to the cops. Thus, an even higher level of protection is mandated under the law.

Once again the law requiring the protection for the whistleblower was clear and spelled out directly by Congress in the obstruction of justice statute: "Whoever knowingly, with the intent to retaliate, takes *any action* harmful to *any person, including interference with the lawful employment or livelihood of any person,* for providing information to a law enforcement authority any truthful information relating to the commission or possible commission of any Federal offense, shall be fined under this title or imprisoned not more than 10 years, or both."

Revealing the identity of the whistleblower is an "action" that is "harmful." Given the fact that the whistleblower works for a secret agency, that revelation would also undoubtedly "interfere" with the whistleblowers' ability to earn a living in a spy agency.

Does this law apply when the interference is committed on social media sites, such as Twitter or Facebook?

In August of 2019, the U.S. Court of Appeals for the Sixth Circuit addressed this very issue. In the case of *U.S. v. Edwards,* three Republican appointed judges (one named to the bench by President Trump) agreed that it does. In a case remarkably similar to the Ukraine whistleblower matter, the judges unanimously found a person who derided a witness on Facebook in federal law enforcement guilty of Chapter 73. Obstruction of Justice 18 U.S. Code § 1513 - retaliating against a witness, victim, or an informant. The defendant in the *Edwards* case called a confidential informant a "rat" and a "snitch ass bitch" on Facebook.

The defendant was found guilty of witness retaliation and sentenced to three months in prison and another three and one-half years of supervised release or home detention. The defendant in the *Edwards* case argued that her Facebook statements did not result in any concrete harm to the confidential informant. But calling out the informant by name on Facebook and instilling fear in the whistleblower, was enough for the court to uphold the guilty verdict on appeal.

The defendant argued that Obstruction of Justice 18 U.S. Code § 1513 - retaliating against a witness, victim, or an informant was being misused, as she was simply engaging in "everyday activity on Facebook." This argument failed. A harm is a harm, regardless if it originates on social media. In the case of the Ukraine whistleblower, where the press is reporting that he or she must be driven to work with armed guards, the fear triggered by exposing his or her identity is real, concrete and actionable under the obstruction laws.

But once again the whistleblower comes up short. It is up to the Department of Justice led by Attorney General William Barr to enforce that law. To date, Barr has not taken any action to protect the whistleblower or prosecute those who are threatening him or her.

Justice for the Ukraine Whistleblower?

On December 28, 2019, President Trump retweeted an article that identified the whistleblower. The entire system designed to protect whistleblowers failed. When the Ukraine whistleblower signed the

Disclosure Form to report an "urgent concern," she or he was promised, in writing, confidentiality. That promise was broken. Privacy Act protections were ignored. The Inspector General Act was undermined. The law prohibiting retaliation was violated by the very person mandated to enforce that law. The Attorney General has sat on his hands while credible evidence of obstruction of justice was published in the national news media, on almost a daily basis.

Will justice sleep forever? This issue is now in the hands of Congress. In November it will be in the hands of the American people.

Copyright Kohn, Kohn & Colapinto, LLP 2025. All Rights Reserved.

National Law Review, Volume IX, Number 365

Source URL:https://natlawreview.com/article/setting-record-straight-legal-protections-ukraine-whistleblower-no-one-volunteers