

## **El Masri v. Tenet (4<sup>th</sup> Cir. 2007)**

---

### **Background Facts**

- Victim of National Security Agency “extraordinary rendition program” or “black rendition program.”
- El Masri is a German citizen of Lebanese descent who was identified by the CIA as a terrorist with associations to Al Qaeda
- Seized in 2003 by Macedonian authorities, but denied a lawyer, German consular, or family visits.
- Blindfolded, beaten, drugged, and interrogated by CIA and German officials, then flown to Afghanistan and placed in solitary confinement at a CIA facility for four months.
- Rice and Tenet admitted that El Masri, after all, was innocent.
- El Masri’s captors agreed that he was innocent, but he remained imprisoned until May 2004, when he was flown to Albania and left on an abandoned road.
- Germany is currently prosecuting El Masri’s German interrogators.

### **Plaintiff’s Legal Arguments**

- Fifth Amendment Due Process: under color of law, defendants held him in U.S. custody, subjected him to treatment that “shocks the conscience,” and deprived him of liberty in the absence of legal process.
- Alien Tort Statute: defendants violated international legal norms by arbitrarily detaining him for a prolonged period and for subjecting him to cruel, inhuman, and degrading treatment.

### **Elements of State Secrets Privilege**

- designed to prevent disclosure of information if
- there is a “reasonable danger”
- that disclosure will reveal military, or diplomatic, or intelligence matters which, in the interests of national security, should not be divulged

### **Three-Part Analysis**

1. Procedural requirements (may be asserted only by the U.S. Government)
2. Information to be protected is a “state secret”
  - No “need” exception or other similar exceptions to other privileges;
  - Necessary deference to judgment and expertise of executive branch and intelligence services;
  - Greater probing required where “need” by party is greater, but no balancing test; once existence of “state secret” is established the privilege is absolute.
3. If privilege applies, how far may the matter proceed?
  - dismissal of case if information would be required to establish prima facie case for plaintiff or element of defense; or
  - dismissal where state secrets form the “very subject matter of a court proceeding” or where “state secrets are so central to a proceeding that it cannot be litigated without threatening their disclosure”

### **“State Secrets” in El Masri**

- There has been mere acknowledgment of the existence of “rendition” program, but the government has never revealed any “central facts” about this case or other operational details of the program, including any specifics about El-Masri’s confinement.
- To prove his claims, El Masri will have to expose how the CIA organizes, staffs, and supervises its most sensitive intelligence operations (including the identity of secret witnesses).
- In every material sense, there are still “secrets” worthy of the court’s protection.
- As held in *Totten* (action for br/K of espionage agreements) “public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated.”

### **Judge’s rulings**

- The United States motion to dismiss is granted. I believe that the government has validly asserted the state secrets privilege.
- The privilege has been asserted by the proper party—the executive department. Further, I find that a state secret is involved that deserves protection in evaluating the claim of the

secret which deserves protection. The CIA's denial or admission of the allegations in the complaint regarding the methods and means employed by the foreign intelligent services of the U.S. and other countries would pose a serious risk of revealing such practices and risk grave injury to national security.

- This case needs to be dismissed to prevent the disclosure of state secrets. There simply are no special procedural mechanisms or safeguards that can be employed to prevent the release of the state secret.
- I realize that dismissal will leave El-Masri with no judicial remedy but his private interests must give way to the national interest to protect state secrets.

## **Hepting v. AT&T Corp. (N.D. Cal. 2006)**

---

- Wire tapping: also known as, telephone tapping, is the monitoring of telephone and internet conversations by a third party, often by covert means. The Electronic Communications Privacy Act of 1986 (ECPA) extends legal protection against wiretapping and other forms of unauthorized interception to oral, electronic, radio, e-mail, cellular telephones, pagers, computer transmissions and communications provided by private communication carriers.
- Data mining: “The application of database technology and techniques-such as statistical analysis and modeling-to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.” GAO Report, May 2004

### **Background Facts**

- Plaintiff filed class action alleging that AT&T collaborated with the National Security Agency to conduct a massive surveillance program, which involved tracking domestic and foreign communication records of millions of Americans
- The Complaint alleges that the President authorized this “data mining” program shortly after Sept 11, 2001 and reauthorized it over 40 times since its inception.
- Alberto Gonzalez admitted to program, but he said that the program was limited to people that the government has a reasonable basis to believe is a member, working with, or affiliated with Al Qaeda.
- Former AT&T employee watched the NSA implement the surveillance system at his work location.
- AT&T issued statements admitting that it would assist the government in classified matters if requested.
- AT&T is the largest telecommunications provider and largest local and long distance provider in the world.

### **Plaintiffs’ Legal Arguments**

- Violation of 1st Amendment of the U.S. Constitution by violating customer’s reasonable expectation of privacy in their communications with AT&T and their ability to exercise free speech and associate privately.
- Violation of 4th Amendment of the U.S. Constitution unlawful search and seizure because ATT and government released information without judicial authorization, probable cause, and/or individualized suspicion.

- Violation of Foreign Intelligence Surveillance Act (FISA). Defendants unlawfully and intentionally engaged in surveillance under color of law without authorization by statute. Defendants disclosed or used the information derived from electronic surveillance, and the problem is ongoing.
- Violation of the Electronic Communication Privacy Act of 1986 (ECPA). Defendants illegally intercepted, disclosed and divulged plaintiff's wire and electronic communications while in electronic storage by AT&T service or while carried by AT&T remote commuting service, and failed to notify plaintiffs of the interception and disclosure. ATT divulged plaintiff's records to a government entity without prior consent.
- Violation of Title VII of the Communications Act of 1934. Defendants willfully divulged the existence, contents, substance, purport and effect and means of communication, without consent, outside authorized means of transmission and reception for the purpose of commercial advantage or private financial gain.

### **“State Secrets” in Hepting**

- “State secrets” necessarily revealed if plaintiffs’ Rule 30(b)(6) deposition allowed to continue, asking about any “government authorization” of data gathering.
  - Applicable even where part of a program had been widely acknowledged; even seemingly “innocuous” information can be damaging to national interests where fits into “mosaic” that a sophisticated enemy of the country could use to learn about US operations
  - Reports in the media are not enough to deprive information of “secret” nature; only government acknowledgment suffices here, and “Neither AT&T nor the government has confirmed or denied the existence of a program of providing telephone calling records to the NSA.”
  - A terrorist who operates with full information is able to communicate more securely and more efficiently than a terrorist who operates in an atmosphere of uncertainty.

### **Judge’s rulings**

- I am going to deny the motion to dismiss in this case.
- In evaluating the assertion of state secret privilege I must examine the information that is sought to determine whether it has already been so publicly discussed and is such public knowledge that its release would not damage national security.
- In deciding that I will consider only reliable public sources of information because to do otherwise would allow persons who wish to obtain secret information to manipulate the process. I have reviewed only public admissions or denials of the government and

AT&T or other telecommunications companies.

- This case is different than the *Totten* and *Tenet* cases. AT&T's assistance in national security is not the kind of secret that state secrets privilege was designed to protect or that terrorists would fail to anticipate. The government has discussed the contours of the program and AT&T has admitted it assists the government in matters of national security when asked.
- I recognize that the United States asserts that the state secrets privilege will preclude evidence necessary for plaintiff to establish a prima facie case or for AT&T to raise a valid defense. At this point, however, I think a dismissal on that basis would be premature. The argument can be evaluated as case proceeds through discovery.
- I think my ruling here recognizes the limits of the state secret privilege. The court is also obligated to take seriously its constitutional duty to fairly adjudicate the disputes that come before it.

### **Background Facts**

- Plaintiffs brought suit against AT&T to challenge the disclosure (versus the interception at issue in *Hepting*) of customer communication records to the NSA. P's assert that AT&T violated the Electronic Communications Privacy Act (ECPA) by knowingly and intentionally releasing (divulging) telephone records (date, time and duration) to the NSA, without statutory authorization or prior consent of the customers, so that NSA could search for patterns that might warrant further investigation. (Data mining)

### **“State Secrets” in Terkel**

- “State Secrets” here applies only to data mining, not interception, and no admitted disclosure by government or by AT&T about this program (interrogatories asking for whether AT&T provided records to government, the legal basis for doing to, entities getting these records, and how many records disclosed).
- Here, AT&T in an “espionage relationship” with government, secrets at the very center of plaintiffs’ claims.
- It would undermine the important public policy underlying the state secrets privilege if the government’s hand could be forced by unconfirmed allegations in the press or by anonymous leakers whose disclosures have not been confirmed.

### **Judge’s rulings**

- I am going to grant the government’s motion to dismiss. The state secrets privilege is applicable here. There has been no public disclosures of the existence or non-existence of AT&T’s record turnover. The application of the privilege prevents the plaintiffs from establishing standing.
- I find that requiring AT&T to admit or deny the allegations that plaintiffs need to prove standing would implicate national security. AT&T’s response might reveal the scope of its program and allow would-be terrorists to tailor their behavior to avoid detection, giving adversaries valuable insight into the government’s intelligence activities. State secrets privilege applies and this case is dismissed on that basis.
- I would note that Plaintiffs may seek relief through the legislative or executive branches, which have equal responsibility to ensure that the law is followed.