Ethical Issues in the Military Commissions

James G. Connell, III
Creighton Law School
March 6, 2014
Disclaimer

I am not speaking on behalf of the United States, the Department of Defense, or the Office of the Chief Defense Counsel. All statements and opinions are my own, and are not based on classified information.
2002: MCO No. 1
2006: MCO struck down in Hamdan I
2006: MCA of 2006
2009: Obama elected
2009: MCA of 2009
2011: al Nashiri prosecution
2012: 9/11 prosecution
ABA Model Rule 1.6(c)

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.

Nebraska did not adopt MR 1.6(c)
§ 3-501.6

Discussion point: different duties in Nebraska?
My view: same duty, but duty of competence rather than confidentiality
Duty to Discover, End, and Remedy

NACDL Opinion 02–01

In general, when an attorney has reasonable suspicion that his or her communications with clients in custody are being monitored by government officials, it is NACDL’s position that the attorney must take affirmative action to safeguard confidential communications. Once either the attorney or client discover that surveillance or monitoring is occurring, the free exchange of information and ideas about the case is immediately chilled, and the Sixth Amendment is violated. Both will fear that confidences have already been discovered or even seized by the government. Accordingly, the criminal defense lawyer has a duty to seek to end the surveillance, discover the true extent of it, and find a remedy for what has already happened. One cannot simply rely upon post hoc use of the exclusionary rule because the harm to the ability of the criminal defense lawyer to adequately defend has already occurred and continues, and it substantially risks infecting the fairness of the trial.

3 separate duties:
prevent future breach
discover extent of breach
remedy prior breach
Meet in gov’t-provided location
Gov’t disguised listening devices as smoke detectors

Discussion point: what monitoring at your jails?
Oct 2011 baseline review of legal materials
12/27/2011 Woods order, required JTF review of legal mail
1/8/2012 Colwell directive, prohibiting use of legal mail
5/5/2012 arraignment
11/6/2013 Legal comms order

Discussion point: who has access to your legal mail?
1/28/13 Third party OCA activated security device
Led to investigation of courtroom sound system

Discussion point: who has access to your courtroom audio?
3/28/13 Govt revealed production of defense emails
4/10/13 Mayberry directive, prohibiting privileged materials over email or network drive
10/1/13 Military judge order
Current interim policy of encryption

Discussion point: what steps do you take to protect your networks and email?
FISA Surveillance

Section 4 - Acquisition and Processing - Attorney-Client Communications (C).

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security

- Civil attorneys
- Criminal charge other than indictment
- Intra-team communications
- Consultations

Clapper denied standing, as attorneys could not show reasonable basis to believe they were being surveilled
Backup Slides
Technological Solutions

OpenPGP Encryption for Webmail

Encryption Wizard

TRUECRYPT
FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION
Duty to Protect Email

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 11-459
Duty to Protect the Confidentiality of E-mail Communications with One’s Client

August 4, 2011

A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.¹