THE FUNDAMENTALS OF COUNTERTERRORISM LAW

Presented by the American Bar Association and Center for Professional Development
The materials contained herein represent the opinions of the authors and editors and should not be construed to be the action of the American Bar Association or Center for Professional Development unless adopted pursuant to the bylaws of the Association.

Nothing contained in this book is to be considered as the rendering of legal advice for specific cases, and readers are responsible for obtaining such advice from their own legal counsel. This book and any forms and agreements herein are intended for educational and informational purposes only.

© 2015 American Bar Association. All rights reserved.

This publication accompanies the audio program entitled “The Fundamentals of Counterterrorism Law” broadcast on March 16, 2015 (event code: CE1503FSS).
# Table of Contents

1. Presentation Slides

2. The Fundamentals of Counterterrorism Law – Chapter 15: Cyberterrorism  
   Professor Thomas A. Marks and Rodney S. Azama

   Colonel Dawn M.K. Zoldi

   W. George Jameson

5. Additional Information
Welcome

The Fundamentals of Counterterrorism Law

George Jameson, President, Council on Intelligence Issues

Thomas A. Marks, Department Head, War and Conflict Studies (WACS) at the College of International Security Affairs (CISA), National Defense University

Dawn M. K. Zoldi, Staff Judge Advocate, HQ US Air Force Academy

Register for more FREE CLE
www.americanbar.org/cle/free_cle.html

FUNDAMENTALS OF COUNTERTERRORISM LAW
ABA WEBINAR
March 16, 2015

W. GEORGE JAMESON
Council on Intelligence Issues
and
Jameson Consulting

Copyright (c) W. George Jameson
February 2015
www.americanbar.org/cle/free_cle.html
Introduction

- Dealing with terrorism both comprehensively and, to the extent possible, in an anticipatory fashion raises many legal and policy challenges.

- The evolution of U.S. policy and application of the laws in dealing with terrorism over the past 20-plus years -- from a “criminal” focus to a “war and national security” focus to a “criminal and war and national security focus” -- has left many confused about the availability and sufficiency of U.S. laws, policies, and capabilities for addressing counterterrorism challenges.

- Critics of US policies and actions and defenders alike assert that it is an open question whether U.S. laws are fully adequate to address the significant challenges the Nation faces in countering terrorism and defending national security while protecting civil liberties and privacy interests.

Framing the Discussion

- Debates over the legality and propriety of national security operations should not be surprising.

- According to a former DCI: “when Americans are afraid, they want CIA to do more; and when not afraid, they think we are doing too much.”

- Topics of public interest include: Authorizations for use of military force; military commissions versus civilian courts; civil liberties questions in using FISA or other authorities to collect intelligence; use of drones in operations; whistleblowing, leaks, and freedom of the press; cyber threats and operations; oversight and accountability.
National Security Framework

- United States Constitution is the starting point for understanding the national security legal authorities, issues, and challenges:

  "We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America." [Preamble]

- The National Security Act in 1947 expressed its post-war goal:

  "In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States. . . ." National Security Act of 1947, Section 2 (50 U.S.C. 401)

Laws and Policies: Core Authorities & Constraints

- Legislative, Executive & Judicial Powers
  - Tensions inherent in our system: Make, execute, interpret the law
  - Explicit constitutional as well as inherent authority
  - Statutes
  - Executive orders, policies, and directives
  - Case law

- First Amendment
  - Speech, transparency and secrecy

- Fourth Amendment
  - Warrantless operations, agent of a foreign power
  - Reasonable expectations of privacy
Designing Counterterrorism Efforts

- When and Why Does the U.S. Act?
  - What are basic principles?

- Where Can the U.S. Operate?
  - Inside versus Outside U.S.

- What Can the U.S. Do?
  - Military, law enforcement, intelligence

- How Does the U.S. Carry Out Its Activities?
  - Jones case, E.O. 12333?

- Who Does What?

Roles: Form & Function

- Multiple US elements and missions
  - Collection, Prevention, Apprehension, Other
  - Law Enforcement, Military, Intelligence, Homeland Security, Other Civilian Entities

- Roles might overlap, but can provide necessary safeguards to protect from the risk of an unduly powerful central organizational entity.
Intelligence and Military

- Title 10 and Title 50 authorities
  - Traditional Military vs. Covert Action
  - Clandestine is not the same as covert
- Coordination and Collaboration
  - Intelligence Reform
  - UBL example

Intelligence and Law Enforcement

- Intelligence and law enforcement interaction is not new
  - FBI counterintelligence efforts -- close but cautious CIA and FBI collaboration
  - National Security Act “proviso” and Executive restrictions in the 1970’s maintained separation
- Fall of “wall” and transformation of FBI provided new foreign intelligence mission
- Justice Department resources for FISA reviews
- Attorney General’s Guidelines
- FBI as an intelligence agency post 9/11
Selected Major Challenges

• Current and Emerging Threats
  ➢ Cyber
  ➢ New Technologies

• Capabilities & Opportunities
  ➢ Unmanned Vehicles, Monitoring Capabilities

• Implications for Civil Liberties Expectations

Copyright (c) W. George Jameson
February 2015

www.americanbar.org/cle/free_cle.html

Cyberterrorism

Dr. Thomas A. Marks, CISA/NDU
Rodney Azama, IRT

16 March 2015
ABA Webinar

Corresponding author: tamarks@aol.com

www.americanbar.org/cle/free_cle.html
**Cyberterrorism**: “The convergence of terrorism and cyberspace.”

Dorothy E. Denning (Georgetown)

---

**“TERRORISM” COMES IN TWO FORMS:**

Terrorism as a METHOD of action
Terrorism as a LOGIC of action


**METHOD** used by insurgents
One tool among many

**LOGIC** used by “pure terrorists”
“Violence as an end unto itself”

It’s in the *JOC Irregular Warfare* (Sep 07)
(different words, of course)
Framing + Narrative → Lawfare central to conflict

Globalization compression of time and space → “New War”
FUSION OF THE TANGIBLE AND INTANGIBLE

Thus “War of the Mind” Salient

- Tactical/Instrumental: leveraging tools of cyber-domain
- Strategic/conceptual: leverages balance or interface between tangible and intangible worlds (seeing no longer believing; believing is seeing)
Tactical/Instrumental

WMD-like Cyberattack

Cyber Communication/-Recruiting

Strategic/Conceptual

Framing: Define the Conflict

Narrative: Create the Story-line
FRAMING: VICTORY OR MASSACRE?

“Confidential United Nations documents acquired by *The Times* record nearly 7,000 civilian deaths in the no-fire zone up to the end of April.” *TimesOnline, 29 May 09*

NARRATIVE
Liberation or Oppression + Repression?
CONFLICT
“MORPHS”

• STRUGGLE CONTINUES
• NEW FORM (“LAWFARE”)
• DIASPORA CENTRAL
• WEST (US, EU) ENABLES

“None can do a Kosovo on Sri Lanka: wrong century, wrong continent, wrong country.” Dr. Dayan Jayatilleka

But in March 2013
UN Condemned SL

ULTIMATE: OWN THE MIND

THE TIMES
The hidden massacre

20,000 civilians were killed in Sri Lanka's final assault on Tamil Tigers
**KONY 2012: FOR GOOD YET...**

“There most viral video of all time.” TIME

---

**Challenge: Cybercrimes, Hacktevism, Cyberespionage**

“Knowledge is Free. We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.”

**CAN BE A PART OF CYBER TERRORISM TACTICALLY BUT KEY IS STRATEGIC**
NOT “NEW” BUT “ON STEROIDS”

MILITARY STRUGGLE

POLITICAL STRUGGLE

CONCLUSION

GLOBALIZATION HAS BEEN A DIRECT CONTRIBUTOR TO GLOBAL WARMING – BOTH WEATHER AND CONTEXT FOR “NEW WAR”
DOMESTIC DRONE LEGISLATION – IMPACTS ON DOMESTIC CT OPS
Col. Dawn M.K. Zoldi, USAF

*Personal views - do not represent USAF or DoD

PROPOSED LEGISLATION
PASSED LEGISLATION

PRIMARY INTERESTS

• PRIVACY*
  • “UNWARRANTED SURVEILLANCE”

• SAFETY
POINT OF COMPARISON

- DOD INTEL OVERSIGHT POLICY
  - COLLECTION
  - RETENTION
  - DISSEMINATION
  - OVERSIGHT

THE CT ANALOGY

- FIND = DETECT / FIX = DETERMINE LOCATION
  - INFORMATION COLLECTION
    - PROHIBITIONS
    - EXCEPTIONS
  - FINISH = ENGAGE (LETHAL OR NON-LETHAL)
    - OPERATIONAL CONSTRAINTS
    - VIOLATION RAMIFICATIONS
<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APPLICABILITY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State/Local</td>
<td>14%</td>
<td>35%</td>
<td>Up 21%</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>43%</td>
<td>State = 32%</td>
<td>Fed = 14%</td>
</tr>
<tr>
<td>Any Person</td>
<td>6%</td>
<td>33%</td>
<td>Up 27%</td>
</tr>
<tr>
<td>Military</td>
<td>10%</td>
<td>21%</td>
<td>Up 11%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROHIBITIONS/EXCEPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warrant</td>
<td>73%</td>
<td>47%</td>
<td>Down 26%</td>
</tr>
<tr>
<td>Danger to Life</td>
<td>83%</td>
<td>35%</td>
<td>Down 48%</td>
</tr>
<tr>
<td>Danger to Property</td>
<td>20%</td>
<td>13%</td>
<td>Down 7%</td>
</tr>
<tr>
<td>Terror Attack</td>
<td>22%</td>
<td>13%</td>
<td>Down 9%</td>
</tr>
</tbody>
</table>
### COMPARISON

<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prohibitions/Exceptions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Response</td>
<td>17%</td>
<td>15%</td>
<td>Down 2%</td>
</tr>
<tr>
<td>Consent</td>
<td>23%</td>
<td>26%</td>
<td>Up 3%</td>
</tr>
<tr>
<td>Fleeing Felon</td>
<td>18%</td>
<td>14%</td>
<td>Down 4%</td>
</tr>
<tr>
<td>Destruction of evidence</td>
<td>11%</td>
<td>9%</td>
<td>Down 3%</td>
</tr>
</tbody>
</table>

### COMPARISON

<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prohibitions/Exceptions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search/Rescue</td>
<td>16%</td>
<td>17%</td>
<td>Up 1%</td>
</tr>
<tr>
<td>Aerial Inspections</td>
<td>6%</td>
<td>17%</td>
<td>Up 11%</td>
</tr>
<tr>
<td>Ops over Public Lands</td>
<td>9%</td>
<td>6%</td>
<td>Down 3%</td>
</tr>
<tr>
<td>Border Monitoring</td>
<td>2%</td>
<td>0</td>
<td>Down 2%</td>
</tr>
</tbody>
</table>
## COMPARISON

<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROHIBITIONS/EXCEPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Judicial Warr Excs</td>
<td>3%</td>
<td>9%</td>
<td>Up 6%</td>
</tr>
<tr>
<td>Nat’l Security Conspiracies</td>
<td>7%</td>
<td>3%</td>
<td>Down 4%</td>
</tr>
<tr>
<td>Organized Crime Conspiracies</td>
<td>7%</td>
<td>3%</td>
<td>Down 4%</td>
</tr>
<tr>
<td>Crime Scene Investigations</td>
<td>6%</td>
<td>3%</td>
<td>Down 3%</td>
</tr>
<tr>
<td>Amber Alerts</td>
<td>4%</td>
<td>1%</td>
<td>Down 3%</td>
</tr>
<tr>
<td>Controlled Substances</td>
<td>1%</td>
<td>0</td>
<td>Down 1%</td>
</tr>
<tr>
<td>Investigations</td>
<td>10%</td>
<td>15%</td>
<td>Up 5%</td>
</tr>
<tr>
<td>CLAUSE</td>
<td>2013</td>
<td>2014</td>
<td>Difference</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>OPERATIONAL CONSTRAINTS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FACIAL RECOGNITION/BIO-METRICS</td>
<td>13%</td>
<td>14%</td>
<td>Up 1%</td>
</tr>
<tr>
<td>NOTICE TO SUBJECT</td>
<td>11%</td>
<td>10%</td>
<td>Down 1%</td>
</tr>
<tr>
<td>DISSEMINATION / RECEIPT</td>
<td>9%</td>
<td>29%</td>
<td>Up 20%</td>
</tr>
<tr>
<td>RETENTION</td>
<td>22%</td>
<td>12%</td>
<td>Down 10%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATIONAL CONSTRAINTS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEAPONS RESTRICTIONS</td>
<td>31%</td>
<td>23%</td>
<td>Down 8%</td>
</tr>
<tr>
<td>MISSION EXECUTION WINDOW</td>
<td>10%</td>
<td>12%</td>
<td>Up 2%</td>
</tr>
<tr>
<td>COLLECTION/MINIMIZATION</td>
<td>17%</td>
<td>22%</td>
<td>Up 5%</td>
</tr>
<tr>
<td>CLAUSE</td>
<td>2013</td>
<td>2014</td>
<td>Difference</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>PROCEDURAL REQUIREMENTS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acquisition Approval</td>
<td>17%</td>
<td>13%</td>
<td>Down 4%</td>
</tr>
<tr>
<td>Reporting</td>
<td>22%</td>
<td>24%</td>
<td>Up 2%</td>
</tr>
<tr>
<td>Documentation After Emer Use</td>
<td>19%</td>
<td>11%</td>
<td>Down 8%</td>
</tr>
<tr>
<td>Public Notice of Ops</td>
<td>10%</td>
<td>5%</td>
<td>Down 5%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PROCEDURAL REQUIREMENTS</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Keeping</td>
<td>4%</td>
<td>5%</td>
<td>Up 1%</td>
</tr>
<tr>
<td>Fully Comply with FAA GUIDELINES</td>
<td>N/A</td>
<td>26%</td>
<td>Up 26%</td>
</tr>
<tr>
<td>Requirements To Adopt New Procedures</td>
<td>N/A</td>
<td>24%</td>
<td>Up 24%</td>
</tr>
</tbody>
</table>
### COMPARISON

<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIOLATION RAMIFICATIONS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal exclusion</td>
<td>54%</td>
<td>50%</td>
<td>Down 4%</td>
</tr>
<tr>
<td>Civil / Admin exclusion</td>
<td>38%</td>
<td>31%</td>
<td>Down 7%</td>
</tr>
<tr>
<td>Derivative evidence</td>
<td>16%</td>
<td>5%</td>
<td>Down 11%</td>
</tr>
<tr>
<td>Civil liability</td>
<td>34%</td>
<td>33%</td>
<td>Down 1%</td>
</tr>
</tbody>
</table>

### COMPARISON

<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>2013</th>
<th>2014</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIOLATION RAMIFICATIONS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equitable relief</td>
<td>24%</td>
<td>10%</td>
<td>Down 14%</td>
</tr>
<tr>
<td>Criminal penalties</td>
<td>43%</td>
<td>37%</td>
<td>Down 6%</td>
</tr>
<tr>
<td>Criminal provisions</td>
<td>22%</td>
<td>24%</td>
<td>Up 2%</td>
</tr>
<tr>
<td>Admin discipline</td>
<td>2%</td>
<td>1%</td>
<td>Down 1%</td>
</tr>
</tbody>
</table>
WAY AHEAD

• THE PRIVATE BAD ACTOR

• 4TH AM IS NOT A “BUFFET”

• HOUSE CLEANING NEEDED
  • DEFINE KEY TERMS
  • MEANINGFUL PROCEDURAL REQUIREMENTS
  • CONSIDER 2ND/ 3RD ORDER EFFECTS

• DOD POLICIES AS Viable TEMPLATE

Epilogue

• Preserving Both Security and Civil Liberties
  • Legality versus Propriety
  • Current law versus what some think it “should” be
  • Inherent tensions in our national D-N-A
  • Differing international and foreign systems & perspectives

• Oversight
  • Authorizations and prohibitions
  • Separation of Powers
  • Civil Liberties & privacy boards

• Challenges ahead
  • Comprehensive approach
  • National consensus
  • Public trust issues

Copyright (c) W. George Jameson
February 2015

www.americanbar.org/cle/free_cle.html
Thank you for joining us

Register now for the upcoming program in the series!

Beyond Criminal: Civil Remedies for Sexual Assault Victims
Kaethe Morris Hoffer
Chicago Alliance Against Sexual Exploitation
Monday, April 20, 2015
1:00 PM – 2:30 PM ET

Register for more FREE CLE
www.americanbar.org/cle/free_cle.html

CLE Credit Request Instructions

Please stay online…
The program evaluation link will appear shortly. Click on the link to take the program evaluation.

After submitting the evaluation, an online request for CLE credit will appear. Fill out this form to receive CLE credit for this program.

©2014. Published in The Fundamentals of Counterterrorism Law, by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association or the copyright holder.
Introduction

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

—Dorothy E. Denning (Georgetown University)¹

Emergence of Cyberterrorism

Cyberterrorism² is a post–Cold War phenomenon. Today, it is often forgotten that in the mid-1980s, the Internet as we recognize it was a military tool and that even the CIA existed primarily in a “hard copy” world. During the Vietnam War, a letter sent from nearly anywhere in the war zone could be delivered and a response received in “just” five days, which was considered extraordinary. Today, we would expect the end of the world if any computer communication function took so much as five seconds.
So revolutionary has been the compression of time and space that all facets of life—certainly warfare—have been affected. Most particularly, the salience of framing and narrative, both intangible qualities that exist symbiotically with speed of dissemination of images and rationalizations, have impacted upon warfare at the strategic level to the extent that we can speak of “new war” as distinct from traditional “war.” Indeed, the traditional domains of warfare—air, land, sea, and space—have been joined in doctrine by a fifth, cyber (sometimes called “virtual terrain”).

If fusion of the tangible and intangible may be seen as a defining characteristic of the post–Cold War world, it can readily be discerned that terrorism acting in the cyber domain will fall into two principal categories: tactical actions or even campaigns that utilize the tools provided by the “world of the net,” and strategic leveraging of the new global context created by the fusion of tangible and intangible worlds. The widespread use of the Internet by terrorist groups instrumentally for attacks, communication, and recruiting would be examples of the first, with construction of campaigns occurring when the resultant “bundles” of tactical efforts become linked efforts in time and space. An example of the second would be a terrorist threat group consciously structuring its strategic approach so that it exists in the two worlds of tangible and intangible space.

It is the first area, the tactical, which draws most attention, particularly the concern that now-routine cyberhacking and cyberwarfare attacks will be executed by terrorist groups in the same manner that traditional violence (e.g., bombs) is used to target the innocent, with the ultimate being a “WMD-like” cyberattack in its consequences (e.g., as portrayed in the film *The Net*). Significantly, the actual instances of such attacks are reported to be few and thus far of a particular quality, denial of service. In contrast, states have engaged in more destructive behavior, notably Russia in its dealing with those countries of the former Soviet Union that have attracted Moscow’s ire, notably Estonia and Georgia, and, more recently (apparently), American and Israeli attempts using the “Stuxnet” cyberworm to slow Iranian nuclear weapons development.

In the second area, the strategic, much less has been discussed, but the results are far more profound. The exploitation of the intangible dimension, using electronic images and narrative—by Hezbollah and Hamas, for instance—has been so adroit as to mobilize tangible capacity, which threatens not only Israel’s strategic war-fighting efforts but, by calling into question its legitimacy as a state, its very existence. In similar fashion, Liberation Tigers of Tamil Eelam (LTTE) remnants have shifted from emphasis upon tangible action (i.e., kinetics), where the group was decisively defeated in the final May 2009 fighting, to lawfare, enabled by an intangible effort conducted almost exclusively in the virtual world. This shift has not only allowed the Tamil self-defined liberation struggle to continue
but has estranged Sri Lanka from its traditional Western supporters and increasingly isolated it on the world stage.\textsuperscript{14}

These cases thrust forth a final point in considering cyberterrorism, the reality—often lost in general discussions on terrorism but integral to Western doctrinal publications—that terrorism itself has two forms when seen from a war-fighting perspective: terrorism as a logic and terrorism as a method (the terminology is that of Wieviorka\textsuperscript{15}). The latter is terrorism as but one tool utilized by the mass mobilization effort of an insurgency, while the former is what the literature once termed “pure terrorism,” that which structurally is estranged from the social base it purports to represent.

The implications for the discussion above are substantial. Utilized by an insurgency, cyberterrorism will manifest itself at all three levels of war, from the tactical through the campaign (i.e., operational art) to the strategic. The insurgent effort will operate in both tangible and intangible dimensions and will unfold along lines of effort that implement a strategic approach. In contrast, cyber actions by a pure terrorist group must necessarily unfold tactically and to an extent in campaigns, with the focus an effort to translate kinetic damage into message and, thus, influence.

\textit{Analytical Considerations}

\textbf{Distinctions in Defining Cyberterrorism}

As noted in the discussion above, cyberterrorism, in its plain face meaning, is terrorism that occurs in the so-called cyber domain, which some sources claim is a corruption of the proper use of “cyber.” Regardless, the definition that introduced the chapter falls well within common understanding and usage. It can readily be seen, however, that such definition pushes forward a number of distinctions that must be made: that between cyberterrorism and cyberwarfare; that between terrorism and cyberterrorism; and that between cyberterrorism and criminality “of the cyber sort.” Each of these will be considered in turn.

Considering the first: Cyberwarfare, as normally considered in the literature, has to do with the actions of states.\textsuperscript{16} In contrast, terrorism of any type has to do with sub-state actors. Cyberterrorism, therefore, as discussed above, can be delimited as either tactical/campaign—the use of cyber-tools in the same manner as any other means available to a terrorist group (e.g., for communications, defenses, attacks)—or as a more strategic approach to war-fighting that leverages the realities and potentialities of the cyber domain.

Two observed realities of the new age of globalization increase the salience of these observations. The first, as most prominently discussed by Rupert Smith in his \textit{The Utility of Force: The Art of War in the Modern World},\textsuperscript{17} highlights that
changes in global realities, from settlement patterns to linkages, result in a situation wherein conflict invariably must be waged as “war amongst the people” (with its numerous legal implications). Simultaneously, this “war,” as per the “Fourth Generation” theorists, notably William S. Lind in a series of articles,\textsuperscript{18} will be characterized by its conflation of state and non-state actors, with any number of the latter emerging with concentrations of power superior to those of actual states. A logical outgrowth of this has been the official adoption by militaries of the notion that conflicts will more often than not be “hybrid,” involving a variety of martial forms, one of which will be terrorism.\textsuperscript{19}

Not stated but manifest is that Chinese and Vietnamese theorists,\textsuperscript{20} in their extensive conceptualization and incorporation into doctrine of, respectively, “political warfare” and “the war of interlocking,” were in some cases at least half a century in advance of such Western discussion. Though the cyber world was not yet in existence, little that is in the Chinese or Vietnamese works requires such specificity. Indeed, applied to the cyber domain, their fusion of tangible and intangible merely becomes more potent.

**Terrorism and Cyberterrorism**

Chinese and Vietnamese theorists thus emphasized half a century ago what for the West emerged as a seminal shift only at the end of the Cold War, the centrality of “human terrain” to all warfare. Any consideration of terrorism has long been more than a little aware of this reality. Terrorism, regardless of permutations—occasioned overwhelmingly by newly emerging states’ historic determination not to be constrained or condemned in wars of national liberation—is today essentially considered to be violence perpetrated against the innocent [persons and property protected by the laws of war] by sub-state actors for the purpose of political communication. Even “religious” terrorism is but a version of this, since the ultimate aims of religious actors are political (i.e., to determine the societal rules of the game, which is a political goal).\textsuperscript{21}

All terrorist actions are attempts to shape facets of the human domain. Tactical cyberterrorism, discussed above, focuses on individuals and property, while the strategic effort extends to the far more profound business evident in the Hezbollah and Hamas efforts: the actual altering of perception to the extent that no state counter can gain traction, much like coating a road with oil. Orwell’s masterpiece, \textit{1984}, comes quickly to mind here, but he was discussing state action, while we are considering sub-state actors.

It is important to reiterate that here we are focusing upon much more than the communication of messages,\textsuperscript{22} as is normally associated with terrorism as “propaganda by the deed.” Rather, we endeavor to call attention to the intangible restructuring of reality to elicit favorable tangible reaction. The critical importance
of framing and narrative stems directly from this reality. Put perhaps offhandedly but accurately, seeing is no longer believing; believing determines what one sees. In the present-world context, terrorists, as armed politicians, have grasped this point as well as any “normal” politicians.23

Such conceptualization brings to the fore the very issue that has mired state policy makers today when dealing with rivals: when can an attack be said to have taken place? If there is an inability to answer definitively such a straightforward question with respect, say, to a well–documented case, such as the recent penetration of numerous political and economic targets by Chinese PLA cyber-units,24 how much greater is the incapacity to discern attacks by non-state actors?25 Noteworthy in this respect are the recent attacks by the “Syrian Electronic Army.” It remains unknown to what extent its attacks, which have attempted to do tangible damage (e.g., attack on the computers of the Haifa water system),26 have been the work of (a) the Syrian government, (b) sympathizers, or (c) sponsored sympathizers—that is, a mix of (a) and (b).27

Taken one step further, how can actual attacks, such as that on Haifa (assuming the perpetrator is a non-state actor), be separated from more indirect efforts, such as those associated with altering the very context from which perception is derived? Such efforts, associated historically with the propaganda tactics and campaigns of fascism, are used to alter the mind (chronicled masterfully, in the case of Hitler and Germany, by Leni Riefenstahl in Triumph of the Will, 193528). Already, the use of cyberweapons to shape frames and narratives is held by many to be merely one facet of democratic discourse.

Europe, for example, perpetuates the artificial boundary between the tangible and the intangible by claiming that Hezbollah consists of separate military (kinetic) and political (nonkinetic) “wings.”29 Not only could nothing be further from reality, but this obscures the actions in the intangible dimension that mold minds so that they are of the same quality as committed fascists. Ironically, while extensive academic (and, at one point in time, operational) work has been done on fascist and communist efforts in this area, little has been done beyond the tactical aspects where terrorist groups are concerned, the most prominent area of research being, of course, the numerous studies dealing with the impact of the Internet upon self-radicalization.30 This misses the far more important area of strategic “perception management.”31

Cybercrimes, Hacktivism, and Cyberespionage

The final distinction that must be made is between cyberterrorism and other forms of cybercriminality. This is particularly important, because a central element of a globalized world is what the appropriate literature has termed the “terror-crime nexus.” Therein, one finds much the same divisions of analysis that have
been highlighted above concerning terrorism itself. At the tactical level, there exist the money-laundering mechanisms which have provided sensational scandals for the media of late, with prominent banks implicated in activities involving terrorist funds (transactions that largely involve use of the Internet). At the strategic level, there is the fusion of criminal fundraising with the very essence of a terrorist organization that one associates with FARC and ELN in Colombia, but increasingly with Hezbollah and those of the Mexican cartels; the latter can be judged to be possibly proto-political even as they remain essentially criminal. The point is that it is not only analytically fruitless but dangerous to separate the cyber elements from any other in such nexus. Wire-transferring illicit funds to be laundered, for example, cannot artificially be separated from more the traditional lugging of bags of cash, even if the tactical means are distinct. Hence cybercrimes, while not “terrorism” per se, are invariably today part and parcel of terrorist group activity, especially financing and resourcing.

More intriguing are the political and proto-political aspects of “Hacktivism.” As well covered in myriad discussions, there are the purely criminal aspects of hacking. Of more interest to us here, at what point do the anarchist sentiments underlying much recent hacker activity assume such political salience that they should be treated as terrorism under the definitional terms of reference, especially the inclusion of property under the key “innocent” term? Certainly the actions of individuals as portrayed in *We Are Legion: The Story of the Hacktivists* rise to the level of political as seen in ecoterrorists or animal rights terrorists. And the lack of cohesive group structure or even common ideological platform does not in any way obviate the reality of terrorism should all elements of the definition be present.

Still, it is the noble sentiments of all three, but especially the hacktivists, that have led to considerable ambiguity, with the Orwell tie-in explicit in the film *V for Vendetta* (from the 1990 graphic novel). The plot of *V for Vendetta*, with a lone-wolf “terrorist” engaged in a struggle against a “fascist” world, summons forth a facet of academic work on terrorism that considers the difficulty of using established terminology and analytical constructs in a context lacking or even devoid of legitimacy. In other words, in a situation that borders on genocide, such as created by the Russians in Chechnya, or the Chinese in Tibet and Xinxiang, or the Britain of *V for Vendetta*, who or what qualifies as “innocent”? If no such category exists—i.e., the state and all who are involved with it are “guilty”—then how does one identify any actor as a terrorist, cyber or otherwise?

Matters are much clearer for this analysis where cyberespionage is concerned. Certainly, spying or its reverse (counterintelligence) can be attached to the actions of terrorists, but normally espionage is thought to be within the purview of states, with similar action by non-state actors simply one more aspect of their criminality.
As noted above, it is in fact cyberespionage as opposed to cyberterrorism which thus far has proved of greatest concern to the present world order and its states.

**Cyberterrorism Trends**

**Globalization, Technology, and the Cyber Environment**

Globalization, though not negating basic parameters or terminology for the analysis of terrorism, has created a “new terrorism,” as oft noted by commentators. In particular, it has turned the effort to communicate politically through the use of violence into a truly worldwide effort, with the targeting of potential and intended audiences rivaling—possibly for the first time in history—the approaches and mechanics of commercial advertising and branding. This, as noted previously, has allowed framing and narrative to emerge as such potent components of any political violence involving or labeled terrorism. On the one hand, threat groups, using the astonishing capabilities inherent to cybercommunications, can theoretically reach a universe of potential sympathizers, supporters, and recruits. On the other hand, they can leverage intangible images and tales of injustice and suffering as any kinetic effort would deploy tangible weapons systems.

The neutralization of Israeli kinetic power during the 2006 Lebanon incursion (discussed previously) is normally held up as the paradigmatic case in this regard, but to this can be added the less effective but nonetheless potent Hamas effort in 2008, as well as the unsuccessful but troubling LTTE tactical effort commencing in 2009 which, in effect, has prevented Sri Lanka strategically from reaping the fruits of a kinetic knockout after nearly three decades of conflict.

In all of these cases, technology was leveraged as weapons system, with intangible “rounds” fired not merely as harassing fire but rather at predetermined targets where they would have maximum tangible impact. The resulting demonstrations and demands for tangible action against Israel and Sri Lanka reached the point, in the latter case, of strategic demands for “humanitarian intervention”—that is, invasion by the international community, as happened in the Balkans (the Kosovo case). In the present, in March 2013, the cyber-dissemination of powerful images of alleged atrocity from the 2009 denouement was used to spearhead a successful United Nations effort at condemning Sri Lanka. Simultaneously, the ruling coalition in India found itself threatened when the same images provoked the withdrawal of a Tamil Nadu partner in the face of New Delhi unwillingness to join the most extreme anti-Colombo positions.

Such efforts have been increasingly enabled by cyber-technological advances which have made the likes of the film *Kony 2012* possible. Analysts have long followed similar, far more sinister efforts orchestrated by terrorist rather than advocacy groups, especially their ability to manipulate digital images before
Cyberterrorism

disseminating the product via the Internet (e.g., YouTube). These are of far greater immediate impact and concern than the much more widely publicized but still hypothetical direct attacks upon critical infrastructure.

Indeed, as maturation of globalization continues, with concurrent leaps in cyberenvironment salience, actions and trends such as this are sure to grow more pronounced. Of most concern is the difficulty of timely, adequate response to well-planned cyber-manipulation that is inherent to the architecture and processes of the cyber world. Sri Lanka again provides a powerful lesson, as the quite successful traditional military blockade of the battle area—a portion of an island, after all—proved incapable of creating a cyberblockade, which allowed LTTE to deliver images on-target and provoke the consequences discussed above. The same may be said of Israel’s effort in Hamas, where it also was able to seal off the battle area in a traditional sense but could not shut down cyberweapons and their consequent tactical and strategic effects.

Actors, Usage, Methodologies

It can readily be seen that several consequences flow from the points just made. First, in an increasingly globalized context, would-be violent political actors can make contact with like-minded individuals. This was well-illustrated by the effort of Anwar al-Awlaki of Al-Qaeda on the Arabian Peninsula, which ultimately involved an astonishing array of actors self-radicalized through, initially, al-Awlaki messages disseminated by the Internet, but later through direct contact. Second, this highlights the extent to which the entire globe now functions in the same manner as the more traditional nation-state area of operations once did. Third, of much greater significance, whereas the state in a traditional counterterrorism or counterinsurgency effort (which necessarily included a counterterrorism campaign) always had to be concerned at the growth of internal challenge and possible external intervention, cyber-enabled processes now can achieve such salience and momentum that they threaten the state itself, as in the Israeli and Sri Lankan cases. This means that any terrorist group with even a modicum of situational awareness will construct its strategic approach informed with just such realities in mind. It is the evidence that this was done in Lebanon 2006 and Gaza 2008 that makes (respectively) the Hezbollah and Hamas cases of such interest.

On the negative side, an interesting consequence of these variable trends is that would-be mass mobilization efforts by insurgents appear to be as yet incapable of escaping the same consequences that have often been noted as resulting from social media—many casual acquaintances but few actual friends. In similar fashion, divorcing the recruitment and sustainment processes of mass mobilization from an actual social base that can achieve critical mass in geographic and temporal spaces can result in isolated, spectacular acts—as seen in the cases of al-Awlaki
recruits such as Umar Farouk Abdulmutallab (the “Underwear Bomber,” convicted in February 2012) or Major Nidal Malik Hasan (the convicted perpetrator in the November 5, 2009, Ft. Hood terrorist shooting)—but thus far has not achieved actual mass mobilization. The impact of social media upon the uprisings that are collectively known as the “Arab Spring” is often held up as showcasing the potential for such action; however, not only has such action eluded the strategies and implementation of terrorists, but the role of cyber acts therein remain contested and not completely understood. The result is that use of the cyber domain for mobilization efforts has paradoxically reinforced the very structural estrangement from the intended social base that is the essence of “terrorism as logic” as distinguished from the mass mobilization of insurgency that is engendered by “terrorism as method.”

Thus, the greatest threat is posed by those groups that can leverage the cyber domain in such manner as to enable strategic approaches that call for use of intangible framing and narrative to mobilize tangible efforts against their foes, normally states. In constructing counters, states are impacted by the usual constraints one associates with any unwieldy bureaucracy: inability not only of timely, appropriate response but of recognition of the challenge that is at hand. Assuming the latter takes place, the challenge is meshing of instruments of national power in such manner as to respond. Depending on the structure and characteristics of the threat group, this is the age-old battle of primary-group dexterity versus secondary-group inertia.

Notes

2. Denning’s definition above is sufficient for our purposes with the critical addition that “terrorism” is executed by sub-state actors, as is presently accepted by all save a minority within academic and policy communities determined to apply the same criteria to states—which is considered by most as so expanding the category as to make it useless for analysis. Our usage therefore is in a sense derivative: cyberterrorism is the use of the cyber domain by terrorists. For further discussion, see Dimitar Kostadinov, Cyberterrorism Defined (as distinct from 'Cybercrime'), INFOSEC Institute Resources, available at http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/.
3. For an engaging discussion, see Ch. 5, The Future of Terrorism, in ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS 151–82 (Alfred A. Knopf, 2013)
4. Our usage here moves beyond the discussion which presently absorbs those concerned with the term directly (i.e., “new war”) or its various permutations (e.g., Fourth Generation Warfare, compound war, hybrid war). Their focus is overwhelmingly on the role of the state or on a synergy of actors and actions (e.g., the use of cyberwarfare in conjunction with state-sponsored irregular warfare). In contrast, we speak to the duality occasioned by warfare that is fought simultaneously in the tangible and intangible worlds—in other words, “on the ground” and “in the
Cyberterrorism

mind." Ironically, it was Taiwan, following the loss of the mainland, which best responded to this new reality. See THOMAS A. MARKS, COUNTERREVOLUTION IN CHINA: WANG SHENG AND THE KUOMINTANG (Frank Cass, 1998), passim.

5. Predictably, terminology remains in a state of flux. U.S. military publications increasingly discuss the “electromagnetic spectrum and cyberspace” or “the EM-Cyber Environment,” even while noting the merging that is taking place. For a particularly useful discussion, see JONATHAN W. GREENERT, IMMINENT DOMAIN, NAVAL INST. PROCEEDINGS 138 (December 2012), 16–21 (Admiral Greenert is the Chief of Naval Operations), available at http://www.usni.org/magazines/proceedings/2012-12/imminent-domain.

6. For useful discussion, see John J. Kane, Virtual Terrain, Lethal Potential: Toward Achieving Security in an Ungoverned Domain, Ch. 3.6 in TOWARD A GRAND STRATEGY AGAINST TERRORISM 252–81.

7. E.g., a strategic communications campaign, which self-evidently is executed through a series of discrete acts that are linked in time and space to form one component of a larger strategic effort.

8. Though Al-Qaeda is perhaps the best-known example, certainly the most effective is LTTE, or the Liberation Tigers of Tamil Eelam (see text below).


13. Numerous sources are now available on this term. For a succinct discussion, see Thomas A. Marks, *Lawfare’s Role in Irregular Conflict*, in *Focus Quarterly* 4 (Special Issue: Counterterrorism), no. 2 (Summer 2010), 12–14, available at http://www.jewishpolicycenter.org/1740/lawfare-irregular-conflict.

14. To our knowledge, there is no single reference on this ongoing LTTE effort; it is discussed briefly in *id*.


20. See Marks, *supra* note 4; therein, the Vietnamese theorists are also discussed, though briefly.


22. This facet of the subject is discussed well in Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (U.S. Inst. for Peace, 2006).

23. A detailed effort to grapple with this point, which perhaps leans too heavily on particular aspects of communications theory but is superb nonetheless, is provided by Jonathan Matusitz in *Terrorism and Communication: A Critical Introduction* (Sage, 2013).


31. *See, e.g., Susan L. Caruthers, Winning Hearts and Minds: British Governments, the Media and Colonial Counter-Insurgency 1944-1960* (Leicester Univ. Press, 1995); or, more recently (though examining a particular facet of the subject), Clifford Bob, *The Marketing of Rebellion: Insurgents, Media, and International Activism* (Cambridge Univ. Press, 2005). Likewise, there is ample material on both sides of the tactical and even operational use of cyberwarfare to further terrorist efforts. On the larger subject of strategic perception management, though, there appears to be as yet no benchmark work. Touching upon the issue in part is Brigitte L. Nacos, *Mass-Mediated Terrorism: The Central Role of the Media in Terrorism and Counterterrorism* (Rowman & Littlefield, 2007); *see especially 113–41.*


33. For an extensive discussion of this larger issue, to which cyber-criminality is now symbiotically linked, *see Jodi Vitto, Terrorist Financing and Resourcing* (Palgrave Macmillan, 2011).

34. Luminant Media (2012), available commercially at (among others) Amazon.

35. At least one excellent review finds so little political in the Anonymous posture that it would no doubt disagree with this conclusion; *see Sue Halpern, Are Hackers Heroes?, N.Y. Review*
OF BOOKS (Sept. 2012), 42–45, available at http://www.nybooks.com/articles/archives/2012/sep/27/are-hackers-heroes/?pagination=false. Halpern’s position, though, would seem at odds with the emerging literature, a perusal of which would perhaps find even the use of “proto” as inadequate in describing the political agenda of at least some hackers. See, e.g., one of the books she reviews: Parmy Olson, WE ARE ANONYMOUS: INSIDE THE HACKER WORLD OF LULZSec, ANONYMOUS, AND THE GLOBAL CYBER INSURGENCY (Little, Brown, 2012); and three she does not: Heather Brooke, THE REVOLUTION WILL BE DIGITISED: DISPATCHES FROM THE INFORMATION WAR (William Heinemann, 2011); Rebecca MacKinnon, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM (Basic Books, 2012); and Andry Greenberg, THIS MACHINE KILLS SECRETS: HOW WIKILEAKERS, CYBERPUNKS, AND HACKTIVISTS AIM TO FREE THE WORLD’S INFORMATION (Dutton, Sept. 2012).


37. Film released by Warner (2006); graphic novel is Alan Moore (Warner Books, 1990); both available commercially at (among others) Amazon.

38. For the point under discussion, see James Hughes, CHECHNYA: FROM NATIONALISM TO JIHAD (Univ. of Pa. Press, 2007), especially Ch. 5, Chechnya and the Meaning of Terrorism, 128–61.

39. Tibet is perhaps the more glaring case, where, over a period of time, violence has systematically eliminated a way of life; see Wang Lixiong & Tsering Shakya, THE STRUGGLE FOR TIBET (Verso, 2009); also useful, despite its having been passed by events in some respects, is Ronald D. Schwartz, CIRCLE OF PROTEST: POLITICAL RITUAL IN THE TIBETAN UPRISING (Columbia Univ. Press, 1994). For Xinxiang, of a number of possibilities, an older text is revealing; see Dru C. Gladney, DISLOCATING CHINA: MUSLIMS, MINORITIES, AND OTHER SUBALTERN SUBJECTS (Univ. of Chicago Press, 2004).

40. Spencer Lamm, V FOR VENDETTA: FROM SCRIPT TO FILM (Universe, 2006). In the story, Britain, following a nuclear war, is ruled by a fascist party (Norsefire), which uses a brutal police state to cow the remnants who have not previously been outright purged. Thus the scenario dovetails well with the cases under discussion.

41. This is certainly the logic of both ecoterrorism and animal rights terrorists, though individuals so labeled would vehemently deny that they fall within the designation “terrorists.” For an overview, see Donald R. Liddick, ECO-TERRORISM: RADICAL ENVIRONMENTAL AND ANIMAL LIBERATION MOVEMENTS (Praeger, 2006); for an alternative position, see Will Potter, GREEN IS THE NEW RED: AN INSIDER’S ACCOUNT OF A SOCIAL MOVEMENT UNDER SIEGE (City Lights Publishers, 2011).

42. For one aspect of this subject, see, e.g., Blake W. Mobley, TERRORISM AND COUNTERINTELLIGENCE: HOW TERRORIST GROUPS ELUDE DETECTION (Columbia Univ. Press, 2012).


45. The video and commentary are available at http://invisiblechildren.com/kony/. Released in March 2012, the film called for the apprehension and trial of indicted war criminal Joseph Kony (originally in Uganda) and rapidly became “the most viral video of all time” [according to Time]. See http://en.wikipedia.org/wiki/Kony_2012.


48. This reality has been so widely demonstrated that analysis has moved on to the more intriguing area of the precise nature of individual interface with mobilization efforts enabled by technology. See, e.g., BRUCE BIMBER, ANDREW FLANAGIN & CYNTHIA STOHL, COLLECTIVE ACTION IN ORGANIZATIONS: INTERACTION AND ENGAGEMENT IN AN ERA OF TECHNOLOGICAL CHANGE (Cambridge Univ. Press, 2012).


51. It is perhaps noteworthy that in Shirow Masamune’s 1989 manga series, The Ghost in the Shell, English trans. (Dark Horse Comics, 2009), the terrorist villain(s) operates by infiltrating the minds of his targets (humans with cyber-brains) and planting alternative worlds therein to lead them into second- and third-order terroristic actions as a consequence of what, in reality, are virtual “memories.” The animated film of the same name was released in the U.S. in 1998 (Palm Pictures); it is available commercially at (among others) Amazon.
I. Introduction

Find. Fix. Finish. Doctrinally, the targeting cycle remains the same, whether the target is located abroad or at home.¹ Yet operations to prevent, counter, or respond to domestic terrorism are different from those overseas in many respects. State and federal law enforcement agencies, not the Department of Defense (DoD), will be the country’s first line of defense for domestic counterterrorism (CT) operations.² Even so, the DoD may be called upon to support law enforcement agencies. What if any one of these agencies planned to use a drone in support of its CT efforts at home?³ For some, this very idea raises the specter of illicit government surveillance—or even more controversial, the extrajudicial killing—of Americans on United States soil.

To allay fears related to privacy and due process, 43 states have proposed 86 drone bills to “protect citizens’ privacy” or free them from “unwarranted” surveillance.⁴ Eight states have already passed such legislation.⁵ Of these state proposals, 90% apply to state and local government actors, primarily to law enforcement agencies.⁶ Forty-one percent also extend their applicability to U.S. or

* The views contained herein are those of the author and should not be attributed to the Department of Defense, the U.S. Air Force, or Air Combat Command.
federal government employees. Twelve percent of state bills directly address the U.S. military, but many more could also apply. Federal drone legislation has also been introduced. These proposals largely track state initiatives and apply to both state and federal actors. In addition, while DoD drone policies apply directly to DoD personnel, they also have indirect effects on the civilian agencies they support. Thus, drone legislation and policies will impact conduct across the range of governmental actors during all operations, but in particular domestic CT operations.

The underlying assumption of this chapter is that states and the Congress will continue to revisit the subject of domestic drone use in relation to privacy and due process until laws are passed. The purpose of this article is to review these legislative drone proposals and policies, explore their potential impact on domestic CT operations and identify best practices that allow drones to be used to their full operational potential in CT operations, while protecting privacy and liberty.

**II. Find and Fix**

Finding a target means detecting it. Fixing the target means determining its positional location. Drones perform both of these functions well. To the extent that proposed drone laws and existing drone policies address using these assets to collect information or evidence about a person, they have implications for “finding and fixing” terrorists domestically. Below is an overview of state and federal drone bills and DoD policies relevant to the “find and fix” aspects of domestic CT operations.

**A. State Legislation—Information Collection**

Almost universally, state drone legislation prohibits the use of drones to collect information or evidence. There are, however, exceptions, the most common being where law enforcement obtains a judicial warrant or court order.

Highly relevant to a domestic CT scenario, 22% of proposed state drone bills permit drone use without a warrant in relation to a terrorist attack. All the state bills that contain a “terrorist attack” exception use similar language: “To counter a high risk of a terrorist attack by a specific individual or organization if the United States Secretary of Homeland Security . . . determines that credible intelligence indicates that there is such a risk.” Although the bills do not define “counter,” the language appears to be preventive in nature, to thwart a likely future or imminent terror attack. The bills also do not define “terrorist attack.” A scan of publicly available DHS documents does not provide an obvious definition of “terrorist attack.” Because the exception always requires a predicate determination by the Secretary of Homeland Security that a high risk of a terrorist attack exists before it can be invoked, the secretary’s interpretation as to what acts rise to the level of a domestic terror attack would be determinative.
Along similar lines, Arkansas, Hawaii, Maine, and Michigan would allow state or federal agencies to use drones for emergencies involving “conspiratorial activities threatening the national security interest.” Like the terror attack exception, the national security interest conspiracy exception contains significant terms that remain undefined, such as “conspiratorial activity” and “national security interest.” As such, these state provisions would be subject to individual interpretation.

Most terror attack scenarios would invoke the potential of immediate danger of death, serious physical injury, or significant property damage. All but 14 states have proposed drone bills to permit their use in a proactive manner to save lives in emergency situations. These provisions are most commonly styled as an “imminent danger to life” exception. Most of these same provisions also permit drone use to prevent property damage.

Other CT-relevant exceptions include provisions that would permit drone use on or over public lands or to monitor borders. Depending on the facts of a particular CT event, state drone legislative exceptions, such as those permitting drones to pursue fleeing suspects, to prevent the destruction of evidence, or to be used in situations tantamount to “judicially recognized exceptions to the warrant requirement,” might also apply. Less relevant in the CT arena, but worth mentioning, fewer than a quarter of drone bills surveyed permit their use where the target or property owner has consented.

Some state drone bills also contain exceptions that would allow drones to be used to mitigate the effects of a domestic terrorist event, including provisions for disaster response and search and rescue (SAR). Other provisions that might be employed after a terror attack include those from Illinois, Oregon, and Texas, which allow drones to assess crime scenes.

In addition to when a drone may be used, many state bills address how they may be used by including time, place, and manner restrictions. These operational restrictions and procedural requirements would impact all operations, including CT. One of the most common time restrictions on drone use is a 48-hour mission execution window. Place restrictions focus primarily on the home and areas surrounding it, farms and agricultural areas, and places of worship. Manner restrictions generally require users to collect information only on the target and to avoid or minimize collection on other individuals or property. For example, Massachusetts, North Dakota, and West Virginia do not allow drone surveillance of citizens exercising their constitutional rights relating to freedom of speech and freedom of assembly.

Many states also restrict how the information collected is used, disseminated, or retained. A number of bills reviewed prohibit use of facial recognition or other biometric matching technology on drone-collected information, primarily involving
non-targets. The Maine bill would not permit use of biometrics even on data related to the target of the collection. Very few bills address dissemination of information beyond the collecting agency. That said, some states require dissemination, in the form of notice, to the subject of the drone monitoring.

On the other hand, the majority of bills address retention. The primary theme in retention is to delete information collected unlawfully or on non-targets within 24 hours of collecting it. Other states have retention limits on information lawfully collected on a target of surveillance, unless it is necessary to maintain it for a criminal investigation or prosecution.

A majority of bills contain extensive documentation, oversight, and reporting requirements. A handful of states require public notice of drone operations, images, and government agency drone reports filed. California and Michigan contain a unique requirement to distinctively mark the body of a drone in some manner.

Finally, state drone proposals contain a wide range of ramifications for violating their provisions, from exclusion of evidence to personal liability. The threat of personal liability, whether civil or criminal, has the potential to impact an operator’s decision-making process during CT operations and merits discussion. More than half of the state bills create civil liability for violators. Many include civil equitable relief, including injunctions, to preclude drone use in advance of employment or to prevent the use of information collected. Bills contain a wide spectrum of potential civil penalties that include actual damages, punitive damages, and even treble damages. Several states create criminal liability, ranging from a simple misdemeanor to felonies. A few bills also provide for administrative discipline. Exclusionary rules will be discussed further in “Section II—Finish.”

B. Federal Legislation—Information Collection

Against this backdrop of state legislative activity, federal legislators have also introduced drone proposals. To a great extent, these mimic state requirements with regards to prohibitions, exceptions, operational restrictions, and violation ramifications.

The Preserving Freedom from Unwarranted Surveillance Act of 2013 is short and simple, similar to several of the state bills. While it would apply to persons or entities “acting under the authority of the United States,” the focus appears to be on law enforcement. As with the majority of state bills, it prohibits the use of a drone “to gather evidence or other information” with the additional caveat “pertaining to criminal conduct or conduct in violation of a regulation.” Also like many state bills, this Act contains a warrant exception, exceptions allowing for patrol of borders, “exigent circumstances,” danger to life, pursuit of fleeing felons, to prevent destruction of evidence, and to thwart imminent terrorist attack.
also allows for civil liability and injunction in the same terms used by most states, “to obtain all appropriate relief to prevent or remedy a violation of this Act.”

Two virtually identical acts, both titled The Drone Aircraft Privacy and Transparency Act of 2013 (DAPTA), have been proposed that would also amend the FAA Modernization and Reform Act of 2012. Both DAPTA bills target specific federal agencies and law enforcement, but their information collection provisions are much broader and apply to “any person or entity.” An expansion on the common provision found in many states, the DAPTA would specifically require a warrant for drone use for intelligence purposes as well as for law enforcement surveillance—with danger to life and terrorist attack exceptions. Procedurally, the DAPTA require filing of the justification for such emergency use with the Secretary of Transportation (SecTrans) within seven days post-flight and the destruction of incidentally collected information.

With regard to specific agency requirements, the DAPTA direct SecTrans, in consultation with several other agency heads, to carry out a privacy study, adopt rules to protect privacy, and require data collection and minimization statements from drone users. These bills also require the FAA to post approved certificates of drone use on a public website.

Of all state and federal bills reviewed, the DAPTA contain one of the most far-reaching ramification schemes. In addition to private civil causes of action against individuals and the government, the DAPTA allow state governments to bring suit on behalf of their residents to enjoin, enforce, seek damages, or obtain other relief. They also contain an exclusionary rule applicable to “any trial, hearing or other proceeding,” including before state courts. The bills also create a new enforcement mechanism pursuant to the Federal Trade Commission (FTC) Act. In cases where drones are not operated consistent with the data collection statement submitted, the FTC may treat this as an unfair or deceptive act or practice. In addition, the DAPTA require mandatory license revocation for noncompliance with data collection statements.

Whereas the DAPTA contain an extensive ramification scheme, of all the federal legislative proposals, the Preserving American Privacy Act of 2013 (PAPA) contains the most extensive overall regulatory schemes. It would apply to U.S. departments or agencies as well as to states. The PAPA takes a nuanced approach regarding the information covered by it as “information that is reasonably likely to enable identification of an individual” or “information about an individual’s property that is not in plain view.”

Similar to the majority of state laws, the PAPA would prohibit operation of a drone to collect or disclose information “for a law enforcement purpose” with the following exceptions: pursuant to a warrant or judicial order; to patrol or secure the border; with consent from the individual about whom the information would be
collected; and in emergency situations, defined as “immediate danger of death or serious physical injury to any person; conspiratorial activities threatening the national security interest or conspiratorial activities characteristic of organized crime.”

The PAPA also contains a host of operational and procedural restrictions similar to state bills reviewed. Federal agencies must obtain a warrant no later than 48 hours after an “exigent circumstances” operation begins. Drone collection pursuant to a court order is limited to a 48-hour execution window, renewable for up to 30 days, and with a 10-day post-operational notice to the subject or a 48-hour pre-operational notice to the public. The Act also contains a 10-day notice requirement to the subject of the collection unless doing so would jeopardize an ongoing investigation. It also contains extensive reporting, in terms similar to state bills, from the Administrative Office of the U.S. Courts and the Attorney General (AG) to Congress. One unique twist to the PAPA is that any collection of covered information requires drone operators to minimize collecting information on non-targets, as well as the filing of a “data collection statement” with the AG, which will ultimately be filed on a publicly available website, along with any federal licenses granted to operate the drone.

The PAPA includes the full gambit of ramifications found in state bills for violating its provisions, including administrative discipline for intentional violations.

Finally, the PAPA states that it should not be construed to “preempt any state law regarding use of unmanned aircraft systems exclusively within the borders of that state.” Thus, if passed, government operators would have to comply with both the PAPA and applicable state law(s).

C. DoD Support of Law Enforcement and Information Collection Policies

As mentioned, although civilian law enforcement agencies will take lead in domestic CT operations, DoD may be called upon to provide support. DoD support to law enforcement agencies is limited by law, including the Posse Comitatus Act (PCA), for fear of military encroachment on civil authority and domestic governance. The PCA restricts direct military assistance for law enforcement purposes except as authorized by the Constitution or Congress. It states:

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined not more than $10,000, imprisoned not more than two years, or both.

For this reason, the DoD has implemented policies pertaining to the provision of support to civilian agencies, including DoDD 3025.18, Defense Support to Civil
Authorities (DSCA). It governs DoD’s provision of temporary support to U.S. civilian agencies for domestic emergencies and law enforcement support.\textsuperscript{70} Most activities or missions involving a drone outside of DoD-controlled airspace require approval from the Secretary of Defense (SecDef) or his delegate, with limited exceptions.\textsuperscript{71} SecDef approval for drone use is explicitly required for DSCA, including support to law enforcement agencies.\textsuperscript{72}

SecDef has concurrently delegated seven specific authorities to the four-star General Officer or Flag Officer commanders of U.S. Northern Command (CDRUSNORTHCOM) and U.S. Pacific Command (CDRUSPACOM) in the Chairman of the Joint Chiefs of Staff (CJCS) DSCA Execute Order (EXORD).\textsuperscript{73} The CJCS DSCA EXORD permits USNORTHCOM and USPACOM to request traditional intelligence resources, such as intelligence, surveillance, and reconnaissance (ISR) platforms that include drones, to conduct DSCA missions. The EXORD applies to domestic incidents, including “actual or potential . . . terrorist attacks.”\textsuperscript{74} SecDef approval authorizes the use of these capabilities for non-intelligence purposes. Once SecDef validates the mission from the primary agency in charge of the incident (e.g., Department of Homeland Security or Federal Emergency Management Agency for domestic terrorism), USNORTHCOM and USPACOM are authorized to provide Incident Awareness and Assessment (IAA)\textsuperscript{75} for situational awareness, damage assessment, evacuation monitoring, and Search and Rescue (SAR); chemical, biological, radiological, and nuclear (CBRN) assessment; hydrographic survey; and dynamic ground coordination.\textsuperscript{76} Should a CT incident occur, several of these authorized purposes would be useful for drone operations, once SecDef approves the mission.

DoD Instruction (DoDI) 3025.21, Defense Support of Civilian Law Enforcement Agencies, must be read in tandem with the DSCA regulation and CJCS EXORD, as it provides additional guidance for DoD support to law enforcement agencies, including sharing information collected during military operations; the use of military equipment and facilities; training; funding; and reporting mechanisms for such support.\textsuperscript{77} The DoDI outlines legal and policy restrictions on DoD support to law enforcement agencies and prohibits the military from interdicting vehicles, conducting searches and seizures, arrests, and similar activities (apprehension, stop and frisk) for law enforcement agencies, as well as engaging in questioning of potential witnesses, using force or threats to do so except in self-defense or defense of others, collecting evidence, forensic testing, and surveillance or pursuit of individuals or vehicles (emphasis added).\textsuperscript{78}

Despite the general prohibition on surveillance, the DoDI specifically authorizes domestic terrorist incident support, upon SecDef approval.\textsuperscript{79} Enclosure 3 to the DoDI states that DoD personnel may be made available to a federal law enforcement agency to operate or assist in operating equipment, to the extent the
Intersection of Domestic Counterterrorism Operations and Drone Legislation

equipment is used in a supporting role, with respect to a domestic CT operation, including support of FBI Joint Terrorism Task Forces.80 This provision implements 10 U.S.C. § 374, which states that SecDef may provide DoD personnel to operate equipment for federal law enforcement agencies with respect to domestic CT operations for purposes of, among other things, “aerial reconnaissance.”81 Although the Act itself does not elaborate, the DoD defines reconnaissance (or RECON) as “[A] mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.” (Emphasis added.)82

In addition to these DSCA and law enforcement-related rules, DoD has an additional set of policies that directly relate to intelligence capabilities’ collection of information on U.S. persons (USPER) that also apply to drone operations.83 Executive Order (EO) 12,333, United States Intelligence Activities, as amended, and its implementing directives and instructions, guides the conduct of intelligence activities within a strict intelligence oversight (IO) framework that balances the need for effective intelligence with the “protection of constitutional rights” through collection, retention, dissemination, and oversight processes.84 Under this framework, when conducting an authorized mission, drones can only collect information on USPER that:

- is obtained with the individual’s consent
- is publicly available
- constitutes foreign intelligence or counterintelligence (FI/CI)85
- concerns potential intelligence sources or agents
- is needed to protect intelligence sources or methods
- is related to threats to or to protect the physical security of IC-affiliated persons, installations
- is needed to protect intelligence and CI methods, sources, activities from disclosure
- is required for personnel security or communications security investigations
- is obtained during the course of a lawful FI/CI or international narcotics or terrorism investigation
- is necessary for administrative purposes
- is acquired by overhead reconnaissance not directed at USPER and is incidentally obtained that may indicate involvement in activities that may violate federal, state, local or foreign laws.86

Under DoD policy, collection of USPER information by intelligence assets “shall be accomplished by the least intrusive means.”87 This means, generally, to
the “extent feasible” that information should be collected from publicly available sources or with the consent of the person concerned. Should publicly available information or consent not be feasible or sufficient, other means of obtaining the information include collection from cooperating sources, through the use of other lawful investigative techniques that do not require a warrant or approval of the AG, or by obtaining a judicial warrant.

Under these IO rules, the approval authority to collect permissible USPER information varies depending on any special collection procedures to be used. Intelligence capability cooperation with law enforcement agencies is addressed in DoD 5240.1-R under Procedure 12, which permits DoD to provide specialized equipment and personnel to federal law enforcement authorities when lives are endangered. As mentioned earlier, SecDef approval is required to use a drone in support of law enforcement agencies, and the type of support DoD can provide does not include “surveillance” in the law enforcement sense. In an intelligence context, physical surveillance is a term of art. It is a specific means of intelligence collection defined as “a systematic and deliberate observation of a person by any means on a continuing basis. . . .” This collection method is authorized only for CI and FI purposes relating to USPER who are present or former employees of the intelligence component, present or former contractors of such components or their present or former employees, applicants for such employment, or contracting or military persons. However, as mentioned earlier, drones can be used under the CJCS DSCA EXORD for IAA and, per 10 U.S.C. § 374, for aerial reconnaissance in support of federal law enforcement agencies.

DoD policy also contains specific guidance on retaining information retrievable by reference to a USPER’s name or other identifying data. If properly collected, USPER data may be retained. Otherwise, with limited exception, USPER information “acquired incidentally” will be retained only temporarily, for no more than 90 days, “solely for the purpose of determining whether that information may be permanently retained under” the DoD procedures. One notable exception is where incidentally acquired USPER information “may indicate involvement in activities that may violate federal, state, local, or foreign law.”

Once properly collected and retained, USPER information may be disseminated only to limited government recipients for the “performance of a lawful governmental function,” including DoD employees and contractors, federal, state or local law enforcement (if the information involves activities that may violate the laws for which they are responsible to enforce), intelligence agencies and authorized Federal Government agencies or foreign governments when pursuant to an agreement with them. Any other dissemination requires approval of the DoD component’s legal office after consultation with the Department of Justice and the DoD General Counsel.
III. Finish

In targeting, “finish” equates to “engage.” The means of engagement depends upon the desired effect on the target and could include either a lethal strike or nonlethal means of incapacitation, such as capture, detention (or incarceration), and, ultimately, prosecution. In the domestic arena, proposed drone legislation addresses both of these means of engagement through provisions that address “weaponized” drones and that exclude data obtained by drones from court. DoD has its own policies on domestic use of weaponized drones.

A. State Armed Drone and Exclusionary Rule Provisions

Most states restrict operators from carrying weapons, or employing weapons from drones, and limit CT target engagement to other means. Almost a third of the proposals specifically preclude equipping a drone with weapons. Of these, several forbid equipping drones with nonlethal weapons. For example, West Virginia contains a unique provision prohibiting the use of drones armed with, “pepper spray, bean bag guns, mace and sound-based weapons.” Oregon is the only state that specifically bans drone operators from “directing a laser.”

Proposed state drone bills impact nonlethal engagement options as well by creating exclusionary rules for violating their provisions. More than half of the state bills contain a criminal exclusionary rule. Slightly more than a third of the bills contain provisions excluding information gathered by drones from civil or administrative hearings. Several contain a “fruit of the poisonous tree” exclusionary rule, which prohibits use of information or evidence derived from information gathered by drones. Montana and Oregon expressly ban the government from including information acquired by drones in an affidavit to obtain a warrant.


In the federal arena, one bill has been proposed solely for the purpose of prohibiting SecTrans, responsible for the Federal Aviation Administration (FAA), from authorizing “a person to operate an unmanned aircraft system in the national airspace system for the purpose, in whole or in part, of using the unmanned aircraft system as a weapon or to deliver a weapon against a person or property.” The No Armed Drones Act of 2013 (NADA), as its name suggests, would amend the FAA Modernization and Reform Act of 2012 to do this. The PAPA, discussed above, also forbids use of weaponized drones.

Three other bills have been introduced to prohibit the use of drones to use lethal force against a person in the U.S. However, all include a significant and CT-relevant exception that allows lethal force to be used if the person poses a threat to life. The Life, Liberty, and Justice for All Americans Act prohibits the
President from using “lethal military force against a citizen of the United States who is in the United States,” including the use of a drone, unless the President determines that:

(1) the individual poses an imminent threat of death or serious bodily injury to another individual; and
(2) using such force will prevent or minimize such deaths or serious bodily injuries.\footnote{110}

\textit{Senate Bill 505 (S.505)}, a bill to prohibit use of drones to kill U.S. citizens in the United States, prohibits “the Federal Government” from using a drone “to kill a citizen of the United States who is located in the United States” unless the individual “poses an imminent threat of death or serious bodily injury to another individual.”\footnote{111} There is no additional requirement that the use of force will prevent or minimize such deaths or injuries. \textit{House of Representatives Bill 1242} contains verbatim language of S.505.\footnote{112}

Whereas the draft bills would allow drones to employ lethal force against a U.S. citizen so long as that person poses an imminent bodily threat, the Obama Administration has stated that the President does not have the authority “to use a weaponized drone to kill an American not engaged in combat on American soil.”\footnote{113} Thus, unless federal law is passed to affirmatively provide that authority, under current policy, a USPER would only be engaged with a weaponized drone domestically if he was considered to be engaged “in combat.”

With regard to nonlethal engagement, several federal bills copy state efforts to exclude drone-collected data if obtained in violation of outlined restrictions. The \textit{DAPTA} bills include an exclusionary rule applicable to any court or hearing—criminal, civil, administrative—regarding information obtained, or information derived from that obtained, in violation of their provisions.\footnote{114} The \textit{PAPA} includes a blanket exclusionary rule, like many states, to prohibit use of information unlawfully collected, “in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof. . . .”\footnote{115}

\section*{C. Department of Defense (DoD) Armed Drone Policy}

Department of Defense Directive 3025.18, \textit{Defense Support of Civil Authorities (DSCA)}, which includes support to law enforcement agencies, states, “Use of armed drones for DSCA operations is not authorized.”\footnote{116} Additionally, the 2006 DepSecDef Memo, \textit{Interim Guidance for Use of Unmanned Aircraft Systems}, states, “Use of armed UAS for domestic HD (homeland defense) or DSCA operations is
Intersection of Domestic Counterterrorism Operations and Drone Legislation

not authorized.” As mentioned above, unless an individual is engaged in combat on U.S. soil, the Obama Administration’s stated position is that the President lacks the authority to lethally target him.\textsuperscript{117} This policy would apply to DoD personnel, as well as other federal officers.

DoD policy does not contain provisions for excluding evidence improperly collected or received from hearings.\textsuperscript{118} Instead, violating DoD IO policies or otherwise engaging in “questionable intelligence activity” which may violate the law, or any such executive order, presidential directive, or applicable DoD policy triggers special notification, investigation, and reporting requirements outside of the Service, to SecDef and, ultimately, to Congress.\textsuperscript{119}

\textbf{IV. Find-Fix-Finish: Domestic Drone Rules as Applied}

To illustrate how this tapestry of state, federal, and DoD drone rules would impact domestic CT operations, consider the following hypothetical situation based on the 2013 Boston Marathon bombings.

\textbf{A. The Facts}

During a renowned running event in X state involving thousands of participants and spectators, two suspects of unknown nationality were identified placing homemade bombs in two different locations. These bombs were made from pressure cookers and contained ball bearings. They exploded 12 seconds apart near the finish line, wounding 180 people. Ten were killed. Civilian witnesses reported sightings of the suspects at different locations in the city. The suspects are considered armed and dangerous. In response, the local law enforcement agency, which possesses a drone, employs it to locate the suspects and to engage them, if necessary. While monitoring the area, the drone’s sensors, which include full-motion video (FMV) capability, detect and capture footage of a robbery in progress, unrelated to the bombing. Given the sheer number of people in the area, the FMV footage also captures images of private citizens as they either try to leave the area or assist in response efforts. The drone eventually locates the suspects running on foot several miles from the scene. Its FMV capability is used to videotape the subsequent law enforcement engagement. The suspects engage in a firefight with law enforcement agencies. The drone is equipped with lethal weaponry, and this capability is used to kill one suspect in defense of other law enforcement personnel on the ground. The other suspect is injured and ultimately prosecuted in state court.

- Was the drone use lawful?
- Could federal or military personnel or assets have assisted?
- Is the evidence obtained against the surviving suspect admissible in a criminal court?
Colonel Dawn M.K. Zoldi

- Can video of the robbers and related testimony be used against them in a criminal trial?
- What should be done with the video containing incidental images of other USPER?

B. State Legislation Analysis

Because Florida, Idaho, Illinois, Montana, Oregon, Tennessee, Texas, and Virginia have all passed drone legislation, testing the hypothetical domestic CT scenario against their provisions provides a realistic illustration of how drone legislation would impact CT operations. Because they are different in so many respects, reviewing each individually demonstrates the type of analysis that would need to be done for any intrastate CT operation. Interstate issues would require analysis of several states’ laws.

1. Florida

The Florida Freedom from Unwarranted Surveillance Act applies only to state or local law enforcement agencies. Although it prohibits local law enforcement from using drones to gather evidence or information, it contains exceptions that allow such use with a warrant, to counter a high risk of a terror attack, to prevent imminent danger to life or serious damage to property, and to forestall the imminent escape of a suspect or the destruction of evidence. It contains a criminal exclusionary rule for evidence obtained in violation its terms. It is silent on the issue of weaponized drones, evidentiary exclusion, and dissemination and retention of information collected.

Under the facts presented, the local law enforcement agency’s use of the drone to find, fix, and lethally engage the target is lawful. Tracking and imaging the suspects without a warrant would qualify as necessary to forestall the suspects’ imminent escape or prevent imminent danger to life. These bases are more reliable than “countering” a high risk of a terrorist attack in this scenario, particularly because the attack has already occurred, and there are no indications the U.S. Secretary of Homeland Security has determined that credible intelligence indicates there is risk of a second attack. With regard to the use of force against one of the suspects, the law does not prohibit the use of weaponized drones. Assuming the use of force in defense of others was otherwise appropriate, the law enforcement agency’s firing bullets from a drone and killing one of the suspects would be justifiable—just as if a police sniper had taken the shot from his rifle while in a helicopter. The law does not impact federal or military actors, and their assistance would be subject to their own authorities and approval procedures.

Because Florida law does not contain a criminal exclusionary rule, even if the drone’s use to collect evidence was somehow deemed unlawful, it does not preclude
the admission of the videotaped pursuit and arrest in criminal court or the testimony of the person who was monitoring. As the language is also silent on information incidentally collected, such as the videotaped robbery, Florida drone law would not preclude its use in court. Finally, because Florida law does not speak to retention of data captured, video containing images of other USPER would likely be handled under Florida’s other privacy or records retention laws.

2. Idaho

The Idaho law adds a new section to Chapter 2, Title 21 of the Idaho Code, Section 21-213, *Restrictions on Use of Unmanned Aircraft Systems*. It prohibits use of a drone “to intentionally conduct surveillance of, gather evidence or collect information about . . . specifically targeted persons” absent a warrant and except for emergency response for safety, SAR, or controlled substance investigations. It applies not only to state agencies, but also to “persons” and “entities.” Like the Florida law, the Idaho law is silent on the issue of weaponized drones, evidentiary exclusion, and dissemination and retention of information collected.

Whether or not the law enforcement agency’s use of a drone in this situation was lawful would depend on the interpretation of the term “emergency response for safety,” which is not defined. However, a manhunt of armed and dangerous fleeing suspects who have just detonated a bomb targeting civilians should reasonably qualify as an “emergency response for safety.” Because the law is broadly written to include “persons” and “entities,” it would apply to federal and military personnel. Their ability to assist local law enforcement agencies would also hinge on the interpretation of “emergency response for safety,” in addition to their internal authorities and permissions.

Assuming the use of force was otherwise valid, the use of lethal force would be considered lawful, given that the law is silent on the issue of weaponized drones.

Because the law does not contain a criminal exclusionary rule, all other things being equal, the video of the arrest, and related testimony, would be admissible. Likewise, because there is no discussion of incidentally collected information, the video would also be admissible as against the robbers. Given the lack of provisions on retention, other Idaho laws might apply to handling the video that contains incidental images of USPER.

3. Illinois

Analysis of the same fact pattern in Illinois would yield results similar to those of Idaho and Florida, with minimal deviation. The applicability of Illinois’ *Freedom from Drone Surveillance Act* is limited to local law enforcement agencies. The law prohibits them from using a “drone to gather information.” However, it...
contains a long list of exceptions: to counter a high risk of a terrorist attack, pursuant to a search warrant, if there is a reasonable suspicion that swift action is needed to prevent imminent harm to life, or to forestall the imminent escape of a suspect or the destruction of evidence, for SAR unconnected to a criminal investigation, for crime scene photography, and of private property with consent. Like Idaho and Florida, the Illinois law is silent on the issue of weaponized drones. However, it addresses evidentiary exclusion and retention and dissemination of information collected.

In these particular circumstances, exceptions for imminent harm to life or to forestall the imminent escape of a suspect would justify law enforcement agencies’ use of a drone. Again, because the attack has already occurred and there are no facts indicating that the Secretary of Homeland Security has made a determination of continuing risk, the terrorist attack exception would ironically not seem to apply. This law also does not prohibit the use of weaponized drones, so lethal action against one of the suspects with a drone would be lawful if it meets other legal criteria for law enforcement’s use of force. The law does not apply directly to federal or military actors or inhibit their ability to assist.

Although the Illinois drone law contains an exclusionary rule, it would not preclude admissibility under these circumstances because the information was not gathered unlawfully. Under its retention provisions, law enforcement agencies must destroy all information gathered within 30 days unless there is reasonable suspicion that the information contains evidence of criminal activity or information relevant to an ongoing investigation or pending criminal trial. Under the latter part of this clause, information pertaining to the bombing suspect and the robbers could both be retained beyond 30 days for use in criminal court. The incidentally collected USPER information, however, would need to be destroyed within 30 days.

4. Montana

The Montana law simply prohibits the admissibility of information obtained from a drone “in any prosecution or proceeding within the state” unless obtained pursuant to a warrant or a judicially recognized exception to the warrant requirement. The law also prohibits use of information obtained by a drone in an affidavit to obtain a warrant unless it was collected pursuant to its own warrant; it would otherwise qualify under a judicially recognized exception to the warrant requirement; or is obtained through the monitoring of public lands or international borders. There are no other provisions.

As discussed in the context of the Florida, Idaho, and Illinois laws, a good case may be made for the application of the imminent danger to life and fleeing felon exceptions. Admissibility of the evidence, whether in the case of the surviving
suspect or the robbers, would hinge on such an analysis. Because the law focuses on the activity, not the actors, it appears to broadly apply to all operators and local law enforcement agencies, federal and military alike. However, the same exceptions to the warrant requirement would apply equally for all of these actors.

The law does not address weaponized drones and thus does not preclude the lethal action taken in this case. Retention of information is also not discussed. USPER information incidentally collected would need to be addressed by resorting to other privacy laws.

5. **Oregon**

Oregon House Bill 2710, *Use of Drones by Law Enforcement Agencies*, applies to local law enforcement agencies and prohibits them from operating a drone, acquiring information through the operation of a drone, or disclosing information acquired through the operation of a drone. Exceptions to these prohibitions include obtaining a warrant, exigent circumstances (person committed a crime, is committing a crime, or is about to commit a crime), written consent, SAR, in emergencies where there is an imminent threat to life and safety, during a governor-declared state of emergency, crime scene reconstruction, and for training purposes.

The law specifically exempts the U.S. Armed Forces from its provisions and is silent on the issue of federal actors. The law prohibits “public bodies” from operating a drone capable of “firing a bullet or other projectile, directing a laser or otherwise being used as a weapon.” Among other things, the law contains a broad exclusionary rule for evidence collected, and evidence derived therefrom, in violation of its provisions. It does not contain provisions on incidentally collected information.

In the instant case, the law enforcement agency’s “finding and fixing” the terrorist suspects was lawful under the exigent circumstances and imminent threat to life and safety provisions because there is reasonable belief that the suspects committed a crime and may be about to commit more. For this reason, the evidence would be admissible against the surviving suspect. However, given the weaponized drone provision in the law, the agency’s lethal action in this case was not sanctioned.

The law does not apply to federal actors and specifically exempts the U.S. Armed Forces from its provisions. Even though it generally prohibits law enforcement agencies from acquiring information from the operation of a drone, acquisition or receipt is allowed under exigent circumstances or where there is an imminent threat to life or safety. Thus, federal and military actors could share information collected with local law enforcement agencies unhampered.
In the absence of a prohibition on using information incidentally collected, video of the robbers would be used against them in a criminal trial if otherwise admissible. USPER information incidentally collected would also be addressed by resorting to other privacy laws.

6. **Tennessee**

Tennessee’s *Freedom from Unwarranted Surveillance Act* also only applies to local or state law enforcement agencies.¹⁴¹ It prohibits them from using a drone except to counter a high risk of a terror attack, after obtaining a search warrant, to prevent imminent danger to life, in searching for a fugitive or escapee, to monitor a hostage situation, and for SAR.¹⁴² The law also states that use of a drone to gather evidence or information constitutes a search under the U.S. and Tennessee Constitutions, and, absent a warrant or judicially recognized exception to that requirement, evidence obtained in violation shall not be admissible in a criminal prosecution.¹⁴³ The law also contains a section on retention. Non-target data must be deleted within 24 hours after collection.¹⁴⁴ The law is silent on weaponized drones.

Applying the Tennessee law to these facts, all activities of law enforcement agencies were appropriate. Use of the drone is justified as preventing imminent danger to life and in searching for a “fugitive.”¹⁴⁵ Because preventing imminent danger to life is an exception to the constitutional requirement for a warrant, the video obtained would be admissible against the surviving suspect. Federal and military personnel or drone assets could have assisted, if approved, as the law applies only to local law enforcement agencies.

With regard to the decedent, the law does not prohibit the use of lethal force. In this case, assuming such force was appropriate to defend the lives of law enforcement personnel on the ground, it was lawful.

Unlike the other laws discussed before it, Tennessee law addresses incidentally collected information. Because it requires that data collected on non-targets be deleted no later than 24 hours after collection, videos of both the robbers and other USPER would have to be destroyed. Ironically, in addressing retention, Tennessee has severely limited the use of collected information for what otherwise would be lawful purposes, such as in a criminal investigation or for prosecution of persons other than the target.

7. **Texas**

The *Texas Privacy Act* is organized differently from the other laws. It contains a large “nonapplicability” section that outlines lawful uses for drones.¹⁴⁶ While it is too lengthy to describe all the nonapplicable drone uses here, several CT-related provisions include: consent; search or arrest warrant; immediate pursuit of a suspect
Intersection of Domestic Counterterrorism Operations and Drone Legislation

(who may have committed an offense greater than a misdemeanor); documenting a crime scene; “for the purpose of conducting a high-risk tactical operation that poses a threat to human life”; on public real property or a person on that property; and as part of an “operation, exercise or mission of any branch of the United States military.” Otherwise, the law is applicable to any person. Such a person commits an offense if he uses a drone to image an individual or private property with “intent to conduct surveillance.” Images illegally obtained as well as those incidentally collected during lawful operations cannot be used in any proceeding or otherwise disclosed. Civil action against violators is also available. The law does not address retention and contains no weaponized drone provision.

Texas law provides multiple bases to use a drone to monitor suspects, including pursuit and high-risk tactical operations exceptions. These exceptions would apply to local and federal law enforcement agencies. The military, on the other hand, would have even more leeway, as the law specifically exempts their missions and operations. As the law contains no prohibitions on the use of weaponized drones, assuming the use of lethal force was otherwise justifiable, it is lawful.

Assuming the initial collection was lawful, the evidence against the surviving suspect would be admissible. However, incidentally collected images of the robbers or other USPER could not be used in trial or otherwise disclosed. As the law does not address retention, presumably other records-retention rules would apply.

8. Virginia

The Virginia law is somewhat unique in that it prohibits local law enforcement agencies’ use of drones before July 1, 2015, unless in support of Amber and similar missing person alerts, for SAR situations involving an immediate danger to the missing person, and to train for those purposes. The law also exempts the Virginia National Guard as well as higher education and research institutions engaging in research and development.

Under Virginia law, finding, fixing, and finishing the suspects is a nonstarter for local law enforcement agencies. Federal and military assets may have been able to employ drones, however. Admissibility of evidence as against both the surviving suspect and the robbers would turn on a Fourth Amendment analysis. Likewise, other privacy laws would regulate the disposition of the video containing incidental images of other USPER.

C. Federal Legislation Analysis

While some federal drone bills closely track state proposals, others contain specific provisions pertaining only to use of force. All apply to federal actors, but some extend their application to states as well. Applying the facts of the hypothetical scenario to these bills yields a wide range of results.
1. The Preserving Freedom from Unwarranted Surveillance Act of 2013

This Act applies only to “persons or entities acting under the authority of the United States” and not to state law enforcement agencies.\(^ {154} \) Under its provisions, federal actors, including the DoD, in this case would be able to gather evidence or other information with a drone under its “exigent circumstances,” danger to life, and “fleeing felon” (forestall imminent escape of a suspect) exceptions.\(^ {155} \) It does not contain a criminal exclusionary rule or address weaponized drones or incidental collection.\(^ {156} \) Thus, this bill would not inhibit federal employees from lawfully collecting information and admitting it into court or using a drone to conduct lethal operations. In fact, for DoD, it would provide affirmative authority to use drones in a surveillance-type role, where current authorities otherwise do not. USPER information incidentally collected would be handled according to other laws and policies.

2. The Drone Aircraft Privacy and Transparency Acts of 2013 (DAPTAs)

The DAPTAs’ collection provisions apply to “any person or entity” and thus to federal, DoD, and state actors.\(^ {157} \) Although the bills generally require a warrant for surveillance, in this case their danger to life exception would apply.\(^ {158} \) As a practical matter, the collecting agency, including law enforcement agencies, would have to file the justification for its emergency use with the SecTrans within seven days after flight.\(^ {159} \) The DAPTAs do not address weaponized drones. While the bills include an exclusionary rule applicable to any court or hearing for information obtained in violation of their provisions, these would not apply because the instant collection was lawful.\(^ {160} \) Under the DAPTAs, information pertaining to the robbers could be retained for use in a criminal prosecution. However, law enforcement agencies would need to destroy incidentally collected USPER information.

3. The Preserving American Privacy Act of 2013 (PAPA)

The PAPA applies to departments or agencies of the U.S. as well as to states, and thus to local law enforcement agencies.\(^ {161} \) Because the Act is not to be construed as preempting state law, all agency operators would have to comply with both the PAPA and applicable state law(s).\(^ {162} \)

Because the PAPA forbids use of weaponized drones, lethal action would not be authorized.\(^ {163} \) Although the PAPA would prohibit operation of a drone to collect or disclose information for a law enforcement purpose, its exceptions for emergency situations include “immediate danger of death or serious physical injury to any person” and “conspiratorial activities threatening the national security interest.”\(^ {164} \) Both of these bases would provide justification to use a drone to pursue the two fleeing terrorists. Before the mission could occur, however, law
enforcement agencies would have to file a “data collection statement” with the Attorney General (AG) and FAA for approval to operate the drone. Law enforcement agencies would have to implement complimentary procedures. After the event, the PAPA would require the agencies to obtain a warrant within 48 hours and provide notice to the subject within 10 days. While these requirements may be consistent with federal law enforcement agency procedures, they do not readily translate into current DoD practice. Assuming all of the above procedures were correctly followed, the PAPA’s blanket exclusionary rule applicable to federal and state courts would not apply.

Even though the PAPA requires drone users to minimize collection of non-target information such as that collected on the robbers in our scenario, it can be retained for criminal prosecution. Other USPER information, however, would have to be destroyed if reasonably likely to enable identification of an individual.

4. The No Armed Drones Act of 2013 (NADA)

This bill would prohibit the FAA from issuing approval to operate a drone in the national airspace system for the purpose, in whole or in part, of using it as a weapon or to deliver a weapon against a person or property. It would impact the scenario insofar as no agency would be able to obtain FAA authorization to use a weaponized drone.

5. The Life, Liberty, and Justice for All Americans Act, Senate Bill 505, and House of Representatives Bill 1242, Bill to prohibit use of drones to kill US citizens in U.S.

The Life, Liberty, and Justice for All Americans Act, which affects only the DoD, allows the President to authorize a military drone to lethally target an American in the United States, but only if that individual poses an imminent threat of death or serious bodily injury to another and using force will prevent or minimize the risk. S.505 and H.B.1242 are identical to the Life, Liberty, and Justice for All Americans Act, with two exceptions: (1) they apply to the federal government (more broadly than just the military) and (2) do not contain the requirement that the use of force will prevent or minimize deaths or injuries. The facts in this case fairly raise the issue of imminent threat and, despite current DoD policy to the contrary, this Act would permit use of lethal force against terror suspects. They would impact the hypothetical case insofar as they would provide affirmative authority for the federal government to employ lethal drones in limited circumstances.
D. DoD Policy Analysis

In the hypothetical scenario, the local law enforcement agency asks for DoD drone support to track fleeing terrorist suspects. Would DoD be able to do this? Under current DoD policy, a request from law enforcement to assist with a drone would be considered DSCA, in particular support to law enforcement agencies, and would require SecDef approval. DoD drones cannot conduct “surveillance” for local law enforcement agencies.\textsuperscript{172} However, as a SecDef approved NORTHCOM mission, drones could be used in a limited manner to assist with dynamic ground coordination and provide situational awareness, subject to IO policies on collection, retention, dissemination, and oversight pursuant to the CJCS DSCA EXORD.\textsuperscript{173} Short of this, only if federal law enforcement agencies became involved and requested DoD specialized assistance could SecDef approve drone use for aerial reconnaissance under 10 U.S.C. 374. Admittedly, neither one of these authorities is a perfect fit for this scenario.

With regard to information collected, SecDef would likely require that IO policies apply to the law enforcement agencies’ support operation. Pursuant to DoD 5240.1-R, DoD drones could be used in support of a federal CT effort, and information pertaining to the person targeted could be retained permanently. Incidentally collected information, such as that on the robber, could be retained temporarily, up to 90 days, and disseminated to local law enforcement for use in a prosecution.

Use of armed drones for DSCA is not authorized.\textsuperscript{174} Even if it were, as mentioned above, unless an individual engaged in combat on U.S. soil, the current Administration’s position is that the President lacks the authority to lethally target him.\textsuperscript{175} Specific statutory authority such as passage of the \textit{DAPTAs} or \textit{PAPA}—or the reality of another catastrophic event like 9/11—might change this policy position.

E. The Key Take-Aways

Applying the facts to a Boston Marathon bomber-like scenario demonstrates that state and federal proposals facilitate drone use for the “find and fix” phases of domestic CT operations more so than the “finish” phase. The application also provides several other key take-aways.

1. \textit{Find and Fix—Define the Exceptions, Add “IO-Like” Protections, Codify DoD Support}

Virtually all state and federal bills reviewed apply to government actors, primarily to law enforcement, and prohibit the use of drones to gather information or evidence absent a warrant or court order, with exceptions.\textsuperscript{176} While on the surface these
Intersection of Domestic Counterterrorism Operations and Drone Legislation

procedures appear to provide new privacy protections, they merely codify Fourth Amendment concepts that already exist.\textsuperscript{177} The most common exception found in drone bills is the warrant requirement, yet to require law enforcement to obtain a warrant before searching for evidence is already well established black-letter law. As illustrated by our hypothetical scenario, during a fast-moving, real-world terror attack it may not be practical to obtain a warrant when time is of the essence. Clearly defining and codifying appropriate exceptions to the warrant requirement will avoid ambiguity and confusion during time-sensitive operations.

a. Define the Exceptions

Most bills permit drone use without a warrant in emergency circumstances to save lives.\textsuperscript{178} This is critical in the CT context, as any terror attack would invoke the potential of immediate danger of death, serious physical injury, or significant property damage. As demonstrated by the hypothetical scenario, these common state exigent circumstances and imminent danger to life exceptions, as well as those in the federal \textit{Preserving Freedom from Unwarranted Surveillance Act of 2013}, the \textit{DAPTAs}, and the \textit{PAPA} proposals, prove very useful in a domestic CT context.\textsuperscript{179} The 14 state bills that currently fail to include an imminent danger exception should reconsider their position on this critical emergency response issue—particularly because the Supreme Court has already endorsed the concept of “exigent circumstances.”\textsuperscript{180}

Although phrased differently, the “fleeing felon” exceptions found in Florida, Illinois, Tennessee, and Texas, and the federal \textit{Preserving Freedom from Unwarranted Surveillance Act of 2013} assisted law enforcement agencies to “find and fix” at-large terrorist suspects.\textsuperscript{181} Despite the prevalence of this exception in bills actually passed and reviewed here, only 16 bills of the 102 surveyed contain this CT-friendly language.\textsuperscript{182} Of those, the only “fleeing felon” language that would not assist CT operations is Wisconsin’s bill, which is phrased as “to locate an escaped prisoner.”\textsuperscript{183} Legislators should seriously consider adding this exception to their bills, given its utility in a domestic CT setting.

Also related to terminology, as demonstrated by application of the Florida, Illinois, and federal \textit{PAPA} bills to our hypothetical fact pattern, the “terror attack” and “national security conspiracy” exceptions would benefit from clarification.\textsuperscript{184} With regard to the former, all the terror attack exceptions are worded the same: “To counter a high risk of a terrorist attack by a specific individual or organization if the United States Secretary of Homeland Security . . . determines that credible intelligence indicates that there is such a risk.” Application of this exception proved difficult in our scenario because the key term “countering,” which seems reactive in nature, has been coupled with the phrase “high risk of a terrorist attack,” which appears prospective. How does one counter what has yet to happen?
A reasonable interpretation is that this exception is preventive. If this is the case, the terror attack exception provides little value where an attack has already occurred. Additionally, in our hypothetical the predicate finding was not present because it was not clear that the U.S. Secretary of Homeland Security determined by credible intelligence that risk of terror attack existed. The lack of such a finding would be the case in a lone- or two-wolf scenario where the problem might be considered local, as opposed to a national one (like 9/11) requiring the full engagement of the National Security apparatus.

Similarly, with regard to the “national security conspiracy” exception, Arkansas, Hawaii, Maine, Michigan, and the federal PAPA all allow state or federal agencies to use drones for emergencies involving “conspiratorial activities threatening the national security interest.” Yet significant terms remain undefined, such as “conspiratorial activity” and “national security interest.” In our hypothetical involving two suspects, basic criminal conspiracy theory might apply. However, at what point does a domestic terror incident become a national security event—a lone-wolf actor involved in a single episode and having limited impact, multiple simultaneous events, or only in a catastrophic 9/11-type attack? Until these terms are defined, even if only by criteria to apply, these terror-related exceptions will continue to miss the mark.

With regard to facilitating CT operations, very few state or federal bills carve out exceptions that would facilitate post-attack recovery, including search and rescue operations, disaster response, or damage assessment. In fairness, these activities should be fairly embraced by an “imminent danger to life” exception, but a better practice would be to provide for these operations explicitly.

b. Add “IO-Like” Protections (Where Needed)

Transitioning from information collection to information handling, most drone proposals fail to address the issues that most directly impact privacy: use, dissemination, and retention. To the extent that current state privacy laws are insufficient to address how law enforcement agencies handles information it collects—regardless of the means of collection—such issues are important to address. Of the eight state bills analyzed in our hypothetical exercise, only two addressed incidentally collected information. The Texas Privacy Act would forbid use or disclosure of incidentally collected information in any proceeding. The Tennessee law goes one step further and requires such be deleted no later than 24 hours after collection, without exception. Both of these laws unduly restrict information that would otherwise be legally available to prosecutors. The drafters of the Illinois law, as well as those for the federal DAPTA and PAPA bills, recognize this by permitting non-target information to be retained if necessary to a criminal investigation or prosecution. These bills track the DoD’s incidental collection
Intersection of Domestic Counterterrorism Operations and Drone Legislation

rules, which also allow retention and dissemination of incidentally collected information relating to criminal acts and are worth repeating. While not addressed by the state laws reviewed in our hypothetical scenario, as discussed earlier, many bills prohibit use of facial recognition or other biometric matching technology on non-target information. If the non-target has committed a crime, such as our robber in the bombing scenario, prohibiting law enforcement agencies from using this valuable identification tool seems unduly restrictive.

c. Codify DoD Support

While DoD IO and drone policies prove useful for protecting privacy in the CT context, for a number of reasons, DoD could benefit from legislation that provides direct statutory authority for drone use in CT operations. DoD’s role in domestic CT is one of support to LEA and is limited by the Posse Comitatus Act (PCA). However, the PCA allows the military to enforce the laws “in cases and under circumstances expressly authorized by the Constitution or Act of Congress.” While the President could use the military in a domestic CT event under his Article II powers, he acts at the zenith of those powers when there is congressional authorization for the action.

Although current policies allow DoD to use drones domestically for IAA and limited aerial reconnaissance, neither one of these bases is the perfect solution for DoD-enabled CT operations in the U.S. Codifying the ability for DoD to employ drones in support of state and local law enforcement agencies’ CT efforts, particularly in situations where local resources are overwhelmed, would alleviate ambiguity and pave the way for partnering more fully, particularly in catastrophic events. Also, given the Obama Administration’s stated position that the President lacks authority to use military force on U.S. non-combatants on U.S. soil, such codification would provide DoD affirmative authority to use drones for CT where none currently exists.

2. Finish—Reconsider Prohibitions

Prohibitions on weaponized drones and excluding evidence where the Fourth Amendment otherwise would not require it has a direct impact on domestic CT operations, as well as significant second- and third-order effects.

Of the eight state drone bills used in the hypothetical scenario, only one addresses weaponization of drones. The Oregon law prohibits “public bodies” from operating a drone capable of “firing a bullet or other projectile, directing a laser or otherwise being used as a weapon.” The federal PAPA and NADA proposals would likewise forbid weaponized drones. The Life, Liberty, and Justice for All Americans Act, Senate Bill 505 and House Bill 1242, acknowledge this by
including an exception that would allow lethal drone action where there is an imminent threat to life or limb.\textsuperscript{197}

Other state and federal bills should follow suit. A drone may very well be the best asset for a particular situation, particularly high-risk tactical situations. The drone can perform the same task as a police helicopter with a sniper on board, but without risking the lives of law enforcement personnel.

Prohibitions on the use of weaponized drones also impact critical training for the military and its partners. For example, in California, Senate Bill 15, which is currently under advisement, states that “an unmanned aircraft system may not be equipped with a weapon.” Doing so is punishable by a fine and imprisonment.\textsuperscript{198} Federal preemption aside, the proposal contains no military exemption, yet California is home to military ranges, bases, and test sites for the Active, Reserve, and Guard components of virtually all the military Services.\textsuperscript{199} Other states, such as Oregon, on the other hand, contain a military exception for all of its provisions, including the weaponized drone provision.\textsuperscript{200} Given the Armed Forces’ statutory duty to organize, train, and equip (OT&E) combat-ready forces, an explicit military exemption like that in the Oregon bill is worth replicating (at a minimum, to avoid unnecessary conflict and litigation).\textsuperscript{201}

The majority of state and federal bills surveyed would also exclude evidence obtained in violation of their drone-related procedures at hearings.\textsuperscript{202} These provisions are problematic on several levels. Aside from being arguably unconstitutional, bills that fail to include the full spectrum of Fourth Amendment exceptions create unnecessary windfalls for criminal suspects. This windfall is not just limited to criminal suspects. States that preclude admission of drone information from civil and administrative hearings extend otherwise inapplicable Fourth Amendment warrant requirements to civil cases.\textsuperscript{203}

Several state and federal drone bills also create civil, criminal, or administrative liability against law enforcement agencies or individual officers for failing to abide by their requirements.\textsuperscript{204} These provisions may very well have a chilling effect on CT operators who will now have to make life-and-death decisions under the added threat of personal liability.

\textbf{V. Conclusion}

Current state, federal and DoD drone proposals and policies facilitate drone use for the “find and fix” phases of domestic CT operations more so than the “finish” phase, across the continuum of potential terror attacks. Regarding the “find and fix” phase, while most drone proposals prohibit information collection, they contain multiple exceptions useful in the CT context, including imminent danger to life and exigent circumstances. Ironically, the two main attempts to statutorily relate drone use directly to domestic CT operations—the “terror attack” and “national
security conspiracy” exceptions—generally miss their mark due to lack of definitional meaning and lack of relevance for localized state attacks not rising to the national level. Although the majority of the state and federal drone bills were introduced to protect privacy, many fail to address critical privacy-related issues, such as dissemination and retention. To the extent that existing privacy laws that already pertain to law enforcement agency–collected information are inadequate, the DoD IO regime bears emulating. On the other hand, the DoD could benefit from legislation that provides affirmative and unambiguous statutory authority for drone use in domestic CT operations to allay Posse Comitatus concerns, among others.

Finally, with regard to the “finish” phase of domestic CT operations, policy makers need to seriously reconsider prohibitions on weaponized drones and rules that require deletion of drone-acquired data, prohibit the use of biometrics, and require exclusion of drone evidence where the Fourth Amendment otherwise would not. Doing so will allow drones to be used to their full operational potential while protecting our security and privacy.

Notes


3. In the robotics industry and within the DoD, drones are typically referred to as “unmanned aerial vehicles” (UAV) or “unmanned aerial systems” (UAS). In 2010, the U.S. Air Force changed the term UAV to “remotely piloted aircraft” (RPA) by institutionalizing RPA pilot training and designating RPA pilots as rated officers (career aviation status). Air Force officials announce remotely piloted aircraft pilot training pipeline, AIR FORCE NEWS, http://www.af.mil/news/story.asp?id=123208561; AFI 11-402, Aviation and Parachutist Service, Aeronautical Ratings and Aviation Badges, Dec. 13, 2010, ¶ 2.2. This change in terminology is significant in that it recognizes that these vehicles are not “unmanned,” but rather are piloted, albeit remotely, by trained and rated officers. However, in everyday parlance, people commonly refer to RPAs as “drones.” For the sake of simplicity, the term “drone” is used throughout this chapter. For an
overview of the various types of drones, from military to commercial off-the-shelf products, the Association for Unmanned Vehicle Systems International (AUVSI) has a searchable database of drone airborne platforms at http://robotdirectory.auvsi.org/UnmannedSystemsandRoboticsDirectory/Home/ (*no endorsement intended or implied).

4. Appendix A outlines pending state drone legislation. Drone legislation and policy is a dynamic issue. Some of these bills have already died in committee, and by the time of publication, more bills will have been introduced. The usefulness of reviewing all bills is to glean trends.

5. FL, ID, IL, MT, OR, TN, TX, and VA have all passed drone legislation. Twenty-four states have introduced two or more bills simultaneously, including AK, AZ, AR, CA, GA, IL, IN, IA, KY, MA MI, MN, NJ, NY, NC, OK, OR, PA, RI, SC, TN, VA, WA, and WV. See Appendix A. CO, CT, DE, LA, MS, SD, and UT have not introduced drone legislation.

6. There are few outliers. The New Hampshire bill was specifically drafted so as “not to impair or limit otherwise lawful activities of law enforcement personnel . . . .” NH HB 619, § 2. One of two Arkansas bills would exempt law enforcement officers and emergency responders operating drones as part of their official job duties. AR SB 1109, § 1, 5-60-3(b)(1)(A)–(B). Michigan and North Carolina would allow drone use if not for an intelligence or law enforcement purpose. MI HB 4455 § 5, ¶ (e) and NC HB 312, § 2(b). Iowa, Pennsylvania, and Virginia prohibit drone use prior to July 1, 2015, with exceptions. IA SF 276, 80C.1., PA SB 875, § 3, and VA HB 2012, 1. § 1.

7. Bills that apply, either directly or by implication, to federal or U.S. government employees tend to use broad terms such as “all persons” or “agents.” See AL SB 317, § 1(2) (applies to “any municipal, county, state, or federal agency the personnel of which have (sic) the power of arrest and perform a law enforcement function); AK HB 159a, § 13(b) (“government employee or agent”); AR SB 1109, § 1., 5-60-106(b)(1)(A)–(B) (would apply to a federal agency, unless acting at the request of a state law enforcement officer or emergency responder); AZ HB 2574, § 13-3007.B. (“unlawful for a person to use drones to monitor . . . .”); CA SB No. 15, § 2(a)–(b), amending § 1708.8 of the Civil Code (“A person is liable . . . .”); GA SB 200, § 4(1); see also GA HB 560, § 2, amending Art. 2 of Ch. 5 of tit. 17, GA. CODE ANN. as 17-5-33(1) and (2) (extends provisions to “a law enforcement officer of any department or agency of the United States who is regularly employed and paid by the United States, this state or any such political subdivision . . . .”); HI SB 783, § 2563B-2(b) (“an agent of the state or any political subdivision thereof, or an individual . . . .”); ID SB 1134, § 1(2)(a) (“no person”); IN SB 20, § 4(a) (“a person”); KY 14 RS BR 1, § 1(1)(c) (“Agent of any prohibited agency”); MA SB 1664, § 1(c) and HB 1357, § 1(c) (apply to “government entities” or “government officials,” without further definition); MI HB 4455, § 1, ¶ (an “individual acting or purporting to act for or on behalf of this (sic) State or local unit of government”); MN HF 990, § 3, Subd. 1(b) (“Person,” defined as any individual); MO HB 46, § 305.637.2. (“No person, entity or state agency”); NJ AB 3929 (“state, local, or interstate law enforcement agency”); NY AO 8091, § 1, ¶ 5 (“he or she”); NY AO 6244, § 1, ¶ 1. (applies to persons or entities acting “under color of the authority of any State, county, municipal or local governmental entity or authority, or acting on behalf of any such entity or authority”); NY AO 4537AO 6370, ¶ 5(C). (includes any “agent of” State or local law enforcement agencies); NY AO 6541, § 66-A(2) (“agent of the state or any political subdivision thereof”); NC HB 312, § 2(a)(2) (“Person—any employee or agent of the United States or any state”); OH HB 207, § 4651.50(A) (“any person acting on behalf of a law enforcement agency”); OK HB 1556, § 3(B)(6), OR SB 853, § 1(2) and MN HF 1620/ 1706, § 3, Subd. 1.(c). (apply, in some manner, to “federal agencies”); OR HB 2710, § 1(1)(b) (police officers are defined to include DoJ criminal investigators); OR SB 71, throughout (“a person”) and OR SB 853, § 2(2)(“a person”); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3.-1.
intersection of domestic counterterrorism operations and drone legislation

(“person” means any individual, partnership, association, joint stock company, trust or corporation, whether or not any of the foregoing is an officer, agent or employee of the United States, a state, or a political subdivision of a state); and 12-5.3-2. (“It shall be unlawful for a municipal law enforcement agency, or any individual or entity on such agency’s behalf, to operate an unmanned aerial vehicle, or to disclose or receive information acquired through the operation of an unmanned aerial vehicle.”); SC HB 3415, amending Ch. 13, tit. 17 of 1976 Code as 17-13-180(A)(2); TX HB 912, Ch. 423, § 423.003(a) (“a person”) and Ch. 423, § 423.002(8) (“a person acting under the direction or on behalf of a law enforcement authority”); WV HB 2732, Art. 7, § 1-7-2 (“law enforcement agency means a lawfully established federal, state or local public agency that is responsible for the prevention and detection of crime.”); WY HB 0242, 7-3-1002(a)(ii) (“federal agency” in their definition of the term “law enforcement agency”); WA HB 1711, § 6 and WA SB 5782, § 2(6) (“‘Person’ includes any individual . . .”); WI AB 203/SB 196, § 3(2) (“whoever”).

8. KY 14 RS BR 1, § 1(4)(b) (permits the “U.S. Armed Forces” stationed in the State to “use drones for purposes of training”); OK HB 1556, § 5.C. and § 4.A (“United States military” permitted to operate “weaponized” drones over public land for purposes of testing and training; “incidental over flight” of private lands allowed while in transit to or from “its destination or base of operation,” if the flight was otherwise compliant with FAA regulations); NJ Assembly No. 3157, ¶ 5 (exempts “any member of the Armed Forces of the United States or member of the National Guard while on duty or traveling to or from an authorized place of duty” from disorderly persons offense for purchasing, owning, or possessing a drone); MO HB 46 § 305.639(2) (permits higher education institutes to conduct educational, research, or training programs in collaboration with the DoD); OR SB 853, § 12(1) (excludes “the Armed Forces of the United States . . . or any component of the Oregon National Guard from using drones during a drill, training exercise or disaster response”); OR HB 2710, § 16 (“passed”) (exempts the “Armed Forces of the United States” from its provisions); PA SB 875, § 5(1)–(3) (exempts its National Guard “during training required to maintain readiness for its federal mission, when facilitating training for other United States Department of Defense units, or when such systems are utilized for the Commonwealth for purposes other than law enforcement, including damage assessment, traffic assessment, flood stages, and wildfire assessment . . .”); TX HB 912, Ch. 423, § 423.002 (“non-applicability” section excludes drone use that is “part of an operation, exercise, or mission of any branch of the United States military”); and VA HB 2012, ¶ 1 § 1 (“passed”) (exempts its National Guard from prohibitions in words verbatim of PA bill above). State bills that broadly apply to any “person” or “entity,” extend their reach to “agents” of State law enforcement, or purport to apply to those acting under State authority would also apply to DoD officials, employees, or personnel.

11. Id., at p. II-25.
12. Drones do not operate without input from a host of professionals, including pilots, sensor operators, and intelligence analysts acting in concert. While a gross oversimplification of a complex system and process, this article uses the same language found in proposed legislation (“drones collect” etc.) with full acknowledgment that it is inaccurate from both a technical and operational standpoint.
13. AL SB 317, § 1(b)(1) (“Except as otherwise provided . . . a law enforcement agency may not use a drone to gather evidence or other information.”); AK HB 159a, amending § 4. AS 1865, Art. 13, § 18.65.900(a) (“Except as provided . . . a government employee or agent, including a police officer, may not participate in an investigation in which an unmanned aerial vehicle is being used, or otherwise directly the use of an unmanned aerial vehicle . . .”); AZ HB
Colonel Dawn M.K. Zoldi

2574, amending § 1, tit. 13, Ch. 30 ARS, 13-3007, § A (“it is unlawful for a law enforcement agency or a state county or municipal agency to use a drone to gather, sort or collect evidence of any type . . .”); AR HB 1904, amending AR Code tit. 12, as 12-19-104(a) (“It is unlawful for a local law enforcement agency to operate an unmanned aerial vehicle or to disclose or receive information acquired through the operation of an unmanned aerial vehicle except . . .”); CA SB 15, tit. 14, § 14352(a) (“a law enforcement agency shall obtain a search warrant to use” a drone) and CA Assembly Bill 1327, § 1, tit. 14, 14350(a) (“a public agency shall not use an unmanned aircraft system, or contract for the use of an unmanned aircraft system, except as provided in this title.”); FL SB 92, § 1(3) (“A law enforcement agency may not use a drone to gather evidence or other information . . .”); GA SB 200, § 5(b) (“An unmanned aircraft shall not be used to conduct a search and seizure except . . .”) and GA HB 560, § 2(b)–(c) (“Any law enforcement agent of the United States/State of Georgia who utilizes an unmanned aerial vehicle for any purpose whatsoever within the airspace of the State of Georgia without first obtaining a warrant shall be guilty of a misdemeanor”); HI SB, 2563B-2(b) (“. . . it is unlawful for an agent of the state or any political subdivision thereof, or an individual . . . to operate an unmanned aerial vehicle or to disclose or receive information acquired through the operation of an unmanned aerial vehicle . . .”); ID SB 1134, § 1., 21-213(2)(a) (“. . . no person, entity or state agency shall use an unmanned aircraft system to intentionally conduct surveillance of, gather evidence or collect information about, or photographically or electronically record specifically targeted persons or specifically targeted private property . . .”); IL SB 1587, § 10 (“Except as provided . . . a law enforcement agency may not use a drone to gather information”); IN SB 20, amending IN Code, Ch. 10, § 4(a) (“A person may not make use of an unmanned aerial vehicle without the written consent . . .”); IA HF 410, § 1. (“A state agency . . . shall not utilize an unmanned aircraft system prior to Jul 1, 2015”) and IA HF 427, § 1.2. (“a law enforcement agency shall not use a drone to gather evidence or other information”); KS HB 2394, § 1(a) (“No law enforcement agency shall use a drone to obtain evidence or other information”); KY HB 454, § 1 of KRS Ch. 500(2) (“Except as provided . . . no law enforcement agency shall use a drone to gather evidence or other information.”) and KY 14 RS BR 1, Sec.1(3)(“no prohibited agency shall use a drone to gather evidence or other information”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4502.2. (“A law enforcement agency may not operate an unmanned aerial vehicle or collect, disclose or receive information acquired through the operation of an unmanned aerial vehicle . . .”); MD HB 1233, 1-203-1(B)(1) (“Except as provided . . . a law enforcement agency may not use a drone to gather evidence or other information . . .”); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(c) and MA HB 1357 (“It is unlawful for a government entity or official to operate an unmanned aerial vehicle except . . .”); MI HB 4455, § 3(3) (“Except as provided . . . a law enforcement agency of this state or political subdivision shall not disclose or receive information acquired through the operation of an unmanned aerial vehicle.”); MN HF 1620/ 1706, § 3, Subd. 2 and SF 1506, § 1, Subd. 2. (“A law enforcement agency may not use a drone to gather evidence or other information on individuals) and MN HF 990, § 3, Subd. 2 (“no person may operate in MN airspace an unmanned aircraft that is equipped with a surveillance device”); MO HB 46, § 305.637.2. (“No person, entity or state agency shall use a drone or other unmanned aircraft to gather evidence or other information pertaining to criminal conduct in violation of a statute or regulation except . . .”); MT SB 196, § 1(1) (“In any prosecution or proceeding within the state of Montana, information from an unmanned aerial vehicle is not admissible unless . . .”); NE LB 412, § (3) (“A law enforcement agency shall not use a drone to gather evidence or other information.”); NJ Assembly No. 3157, § 2.b. (“No law enforcement agency or officer shall utilize an unmanned aerial system unless . . .”) and NJ AB 3929, l.b. (“. . . to conduct surveillance or to gather any evidence or engage in any other law enforcement activity . . .”); NM SB 556, § 3.A.–B. (“A person or state agency shall not
use a drone or unmanned aircraft to gather evidence or other information pertaining to criminal conduct . . . except . . .”); NY AO 6370/ SO 4537, § 1, S 52-A.1. ("No law enforcement agency or a state, county or municipal agency shall use a drone or other unmanned aircraft to gather, store or collect evidence of any type, including audio or video recordings, or both, or other information pertaining to criminal conduct . . . except . . .”), NY AO 6244, § 1. S 700.16, ¶ 1 ("No person or entity acting under color of the authority of any state, county, municipal or local governmental entity or authority . . . shall use, operate, engage or employ an unmanned aerial vehicle . . . to gather evidence or other information related to a criminal investigation . . . except . . .") and NY AO 6541, § 66-A.2 ("except as provided . . . unlawful for an agent of the state . . . to operate an unmanned aerial vehicle, or to disclose or receive information acquired through the operation of an unmanned aerial vehicle . . ."); NC HB 312, § 15A-232.(b) ("Except . . . it shall be unlawful for any person or municipal, county, or State law enforcement agency to use a drone for the purpose of gathering evidence or other information or data pertaining to criminal conduct or conduct in violation of a statute or a rule") and NC SB 402, § 7.16(c) ("no State or local government entity . . . may . . . operate an unmanned aircraft system or disclose personal information about any person acquired unless . . ."); ND HB 1373, § 2.1. ("Except . . . a law enforcement agency may not use an unmanned aircraft for surveillance of a person with in the state or for the surveillance of personal or business property located within the borders of the state to gather evidence or other information pertaining to criminal conduct . . ."); OH HB 207, § 4561.50(A) ("no law enforcement agency, or any person acting on behalf of . . . shall operate a drone in order to obtain evidence or any other information, except . . ."); OK HB 1556, § 3.A. ("Except . . . it shall be unlawful to operate an unmanned aerial system for or in connection to surveillance within the state."); OR HB 2710, § 3.(1) and OR SB 524, § 1(2) ("A law enforcement agency may use a drone for the purpose surveillance of a person only if . . ."); OR SB 71 ("A person may not possess or control a drone unless . . ."); OR SB 853 § 2(1) ("Except as otherwise provided . . . a public body may not operate a drone, acquire information through the operation of a drone or disclose information acquired through the operation of a drone."); PA HB 961, amending Ch. 57 of tit. 18 of PA. CONS. STAT., Subch. E.1., § 5776(a) permits the Pa. Att’y Gen. to submit an application to the court to use a drone in criminal investigations, pursuant to Pennsylvania’s “wiretap” provisions; RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3.-2. ("it shall be unlawful for a municipal law enforcement agency, or any individual or entity on such agency’s behalf, to operate an unmanned aerial vehicle, or to disclose or receive information acquired through the operation of an unmanned aerial vehicle") and RI LC00564, § 1, § 12-5.3-2(a) ("a law enforcement agency . . . shall first obtain a warrant prior to utilizing a UAV"); SC H 3415, amending Ch. 13, tit. 17 of 1976 Code as 17-13-180(b) ("a law enforcement agency may not use a drone, or other substantially similar device, to gather evidence or other information in this State without a legally issued search warrant."); and SC GA Bill 395, § 1, § 6-39-30(A) ("no law enforcement agency may conduct general surveillance or conduct surveillance of a targeted person or location utilizing an unmanned aerial vehicle"); TN HB 591, § 1(c) ("Notwithstanding any law to the contrary, no law enforcement agency shall use a drone to gather evidence or other information.") and TN SB 470, § 1(c) ("Except as provided . . . no law enforcement agency shall use a drone to gather evidence or other information"); TX HB 912, Ch. 423, § 423.003(a) ("A person commits an offense if the person uses or authorizes the use of an unmanned vehicle or aircraft to capture an image without the express consent of the person who owns or occupies the real property captured in the image."); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as § 4622(a) ("Except . . . a law enforcement agency shall not use a drone for any purpose or disclose or receive information acquired through the operation of a drone."); WA HB 1771, § 3, and WA SB 5782, § 3 ("Except . . . it shall be unlawful to operate a public unmanned
Colonel Dawn M.K. Zoldi

aircraft system or disclose personal information about any person acquired through the operation of a public unmanned aircraft system.

A law enforcement agency may not use a drone to gather evidence or other information.

Except as otherwise provided . . . a law enforcement agency may not use an unmanned aircraft for surveillance of a person within the state . . .

WI SB 196/AB 203, § 2, 175.55(2) (“No Wisconsin law enforcement agency may use a drone to gather evidence or other information in a criminal investigation without first obtaining a search warrant.”);

WY HB 0242, 7-3-1003 (“Except . . . a law enforcement agency shall not use a drone to gather evidence or other information pertaining to criminal conduct . . .”).

Two states specifically allow drone use if not for an intelligence or law enforcement purpose:

MI HB 4455 § 5, ¶ (e) (“if no evidence derived from the operation is admitted into evidence . . . or [used] for any intelligence purpose”) and NC HB 312, § 2(b) (“A person or municipal, county, or State law enforcement agency may use a drone for purposes other than gathering evidence”).

Three others, Iowa, Pennsylvania, and Virginia, prohibit drone use, with limited exceptions, prior to July 1, 2015. See IA SF 276, 80C.1., PA SB 875, § 3 and VA HB 2012, 1. § 1.

Besides Iowa, Pennsylvania, and Virginia, which prohibit drone use until 2015, only Indiana, Nebraska, and one of the New Jersey and West Virginia bills fail to include a warrant exception.

The crux of the Indiana bill is obtaining consent. IN SB 20, § 4(a). The Nebraska bill prohibits law enforcement from using a drone to gather evidence and does not contain a warrant exception. It does, however, include a “terrorist attack” exception. NE LB 412, § 4. Although neither NJ AB 3929 nor WV HB 2948 contains a warrant exception, they both permit drone use for terrorist attacks.

ME SP 72, § 4503.1.A.(1)-(2) contains an emergency enforcement exception for threats to national, state, or local security. KS HB 2394, § 1(c) and WV HB 2732, § 1-7-4 require a warrant to use a drone in terrorist attack scenarios.

The DHS electronic publication, Definition of Terms, does not contain a definition of “terror,” “terrorism,” “domestic terrorism” or “attack;” nor does the DHS Risk Lexicon—2010 Edition. See http://www.dhs.gov/definition-terms#top and http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, respectively. However, the latter contains examples of domestic terror attacks in its discussion of “attack method” and “attack path.” These include weaponization of an aircraft and a car bombing involving dozens of individuals moving money, arms, and operatives from the terrorist safe haven to the target area. DHS Risk Lexicon, p. 8. However, JP 1-02 defines “terrorism” as “[t]he unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political.” JP 1-02, p. 80.

All the “conspiratorial activities” threatening a national security interest also include “conspiratorial activities characteristic of organized crime”: AR HB 1904 § 12-19-104, ¶ (a)(2)(i)(a); HI SB 783 § 1, ¶ 263B-4(1); ME SP 72 § 4504, ¶ 1(A); and MI HB 4455 § 9, ¶ 1(a).

Joint doctrine defines “national security interest” as “the foundation for the development of valid national objectives that define United States goals or purposes.” JP 1-02, p. 191. The U.S. National Security Strategy (NSS) describes the full range of threats and hazards to the homeland
Intersection of Domestic Counterterrorism Operations and Drone Legislation


19. Bills that do not contain an imminent danger to life exception include: AK HB 159a; AZ HB 2574; GA HB 560, IN SB 20; KS HB 2394; MT SB 196; NE LB 412; NJ AB 3157; OR SB 71; PA HB 961; RI LC00564; SC GA Bill 395; WV HB 2732; and WV HB 2948. A West Virginia bill and the Kansas bill would allow drones to be used for purposes of an “imminent terrorist attack,” but only after obtaining a warrant. KS HB 2394, § 1(c) and WV HB 2732, § 1-7-4.

20. For “danger to life” exceptions, see AL SB 317, § 1(b)(2)(c) (“prevent imminent danger to life”); AR HB1904, amending AR Code tit. 12, as 12-19-104(a)(2)(A)(i)(a)(1) (“immediate danger of death or serious physical injury to a person”); CA Assembly Bill 1327, § 1, tit. 14, 14350(c)(1) (“imminent threat to life . . .”) and CA Senate Bill No. 15, § 5, amending 14352 of Penal Code, ¶ (b) (“exigent circumstances”—undefined); FL SB 92, § 1(4)(c) (“swift action is needed to prevent imminent danger to life . . .”); GA SB 200, § 5(e)(1) (“imminent danger to life or bodily harm . . .”); HI SB, 2563B-4(1)(A) (“. . . immediate danger of death or serious physical injury to any person . . .”); ID SB 1134, § 1.21–213(2)(a) (“. . . emergency response for safety . . .”); IL SB 1587, § 15(3) (to prevent imminent harm to life . . .”); IA SF 276 (“necessary to protect life, health . . .”), IA HF 410, § 2.c. (“during search and rescue operation if . . . necessary to protect life, health”), and IA HF 427, § 3.c. (“to save a person”); KY HB 454, § 1 of KRS Ch. 500(3)(c) (“. . . swift action is needed to prevent imminent danger to life . . .”); ME SF 72, amends § 1, 25 MRSA Pt. 12, § 4503.1(A)(3) (“threatens life or safety of one or more persons”); MD HB 1233, 1-203-1(B)(2)(II) (“respond to an emergency . . .”); MA SB 1664 and MA HB 1357§ 1, amending Ch. 272 of GEN. LAWS as 99C(c)(3) (“reasonable cause to believe that a threat to the life or safety of a person is imminent . . .”); MI HB 4455, § 5(b) (“. . . reasonable to believe that there is imminent threat to the life or safety of a person.” All MI exceptions apply only to public property. All imaging of private property requires a warrant); MN HF 1620/1706, § 4, Subd. 3(3), MN SF 1506, § 1, Sub 3. (“prevent imminent danger to life”), and MN HF 990, § 1, Subd. 4(5) (“by a public safety agency to prevent imminent serious bodily harm or loss of life”); MO HB 46, § 305.639.1. (“swift action to prevent imminent danger to life is necessary”); NJ AB 3157, ¶ 1.d. (emergency . . . that endangers the public health, safety, or wellbeing of the citizens and residents of this State”); NM SB 556, § 4. (“reasonable suspicion that, under particular circumstances, swift action is necessary to prevent imminent danger to life”); NY AO 6370/ SO 4537, § 1, S 52-A-1. (reasonable suspicion that swift action is necessary to prevent imminent danger to life) and NY AO 6541, § 66-A.3.(B) (“imminent threat to the life or safety or a person”); NC HB 312, § 15A-232.c.(3)(i) (“imminent danger to life”); ND HB 1373, § 3.2. (“reasonable suspicion that absent swift preventative action, there is an imminent danger to life or bodily harm . . .”); OK HB 207, § 4561.50(A)(3) (“to prevent imminent harm to life”); OR HB 1556, § 3.B.3. (“when conducting a search for a mission person, provided it is reasonable to believe that there is an imminent threat to the life or safety of the person”); OR HB 2710, § 1.2.(b) (“risk of serious physical harm to an individual . . .”); OH HB 524, § 1(2)(b) (“emergency situation in which there is risk of serious physical harm to the individual”), and OR SB 853, § 6(1) (“imminent threat to life or safety of the individual”); PA SB 875, § 4 (“during a search and rescue operation if the deployment is necessary to protect life, health”); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12–5.3–2.(f)(1) (“imminent threat to the life or safety of that person”); SC H 3415, amending Ch. 13, tit. 17 of 1976 Code as 17-13-180(B)(3) (“prevent imminent danger to life”); TN HB 591 and TN SB 796, § 1(1) (“necessary to prevent imminent danger to life”); TX HB 912, Ch. 423, § 423.002(a)(12) (“. . . rescuing a person whose life is imminent danger”); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as
§ 4622(b)(2) ("emergency circumstances . . ."); and WA HB 1771, § 9.(1)(a) and WA SB 5782, § 8(1) ("... immediate danger of death or (serious) physical injury to any person"); however, requires grounds upon which a warrant could be entered to authorize the operation; WV HB 2997, § 1-7-3(a) ("imminent danger to life or bodily harm") and WI SB 196/AB 203, § 2, 175.55(2) ("to prevent imminent danger to an individual"); NH HB 619 does not contain an explicit "danger to life" exception but its bill was written so as not to be "construed to impair or limit any otherwise lawful activities of law enforcement personnel." See § 2.V. Even though the following do not contain an explicit "danger to life" exception, other provisions would fairly embrace it: AR SB 1109 (permits law enforcement to use drones for any purpose) and NY AO 6244 (permits lawful exceptions to the warrant requirement).

21. Danger to property provisions include: CA AB 1327 § 14350, ¶ (d)(2) ("court order shall not apply in circumstances involving an imminent threat to persons or property"); FL SB 92 § 1, ¶ (4)(c) (drone use not prohibited if reasonable suspicion exists that "swift action is needed to prevent... serious damage to property"); GA SB 200 § 5(c)(2) (protection of property is an "exigent circumstance" granting law enforcement use of drones); IL SB 1587, § 15, ¶ (3) ("to prevent... serious damage to property"); IA HF 410, § 1.2.c. (protection of property as part of SAR) and IA HF 427, § 1.2.c. ("prevent serious damage to property"); KY HB 454 § 1, ¶ (3)(c) ("needed to prevent... serious damage to property"); MD HB 1233 § 1-203, ¶ (B)(II) ("Respond to an emergency"); MN HF 1620 § 3, Subd. 4, ¶ (3) and MN HF 990, § 3, Subd. 4(5) ("prevent... serious damage to property"); NC HB 312 § 2(c)(3) ("immediate action is needed to prevent... serious damage to property"); ND HB 1373 § 3.3. ("... to... protect property"); OH HB 207, § 4561.50(A)(3) ("prevent serious damage to property"); SC H3415 § 2, ¶ (B)(3) ("prevent... serious damage to property"); OR HB 853, § 8(1) (to protect property during declared emergency); PA SB 875, § 4 (protect property); and TX HB 912 § 423.002 (contains numerous "non-applicability" paragraphs aimed at protecting property including utilities, oil wells, vegetation, etc.).

22. Public land exception bills include: AK HB 159 § 2, ¶ (b)(3) ("to monitor public land"); AZ HB 2574 § 1, ¶ D(2) (law enforcement actively engaged in enforcement on public lands); IL SB 1587 § 15, ¶ (5) ("on lands, highways, roadways, or areas belonging to this State"); MI HB 4455 § 9(1) ("shall only... target public property"); MT SB 196 § 2, ¶ (2)(B) ("to monitor public lands"); OK HB 1556 § 3(3)(B) ("when conducting exclusively on public land"); and TX HB 912, Ch. 423, § 423.002(a)(15)–(16) ("without magnification or other enhancement from no more than six feet above ground level in a public place of public real property or a person on that property"). OK allows drones to transit public land (overflight), including for military aircraft carrying weapons. OK HB 1556, § 4.A. AK and TX, which permit drone use over public lands, also allow their use to monitor borders. AK HB 159 § 2, ¶ (b)(3) and TX HB 912, Ch. 423, § 423.002(a)(14). Other states that allow drone border monitoring include NYS 4537 § 1, ¶ A(3), and ND HB 1373 § 3, ¶ 1.

23. Sixteen bills include a "fleeing felon" exception, which would allow law enforcement officers to pursue suspects or escaped prisoners: AL SB 317 § 1, ¶ (a)(2)(c) ("to forestall the imminent escape of a suspect"); CA AB 1327, § 1, tit. 14, § 14350(c) ("hot pursuit" where there is "imminent threat to life") and CA HB No. 15, amending PENAL CODE § 14352(b) ("exigent circumstances"); FL SB 92 § 1, ¶ (4)(c) ("to forestall the imminent escape of a suspect"); IL SB 1587 § 15 (3) ("to forestall the imminent escape of a suspect"); KY HB 454 § 1, ¶ 3(c) ("to forestall the imminent escape of a suspect"); IA HF 427, § 1.3.c. ("prevent the imminent escape of a suspect"); MN HB 1620 § 1, Sub. 3 ("to forestall the imminent escape of a suspect") and MN HF 990, § 3, Subd. 4(5)(iii) ("prevent the imminent escape of a suspect"); NC HB 312 § 2, ¶ (c)(3)(iii) ("prevent the imminent escape of a suspect"); OH HB 207, § 4561.50(A)(3)
Intersection of Domestic Counterterrorism Operations and Drone Legislation

(“forestall the imminent escape of a suspect”); SC H 3415, § 2, ¶ (B)(3) (“to forestall the imminent escape of a suspect”); TN SB 796, § 1(d)(4) (“searching for a fugitive or escapee”); TX HB 912, Ch. 423, § 423.002(8)(A) (“in immediate pursuit of a person law enforcement officers have probable cause to suspect has committed a felony”); WI SB 196/AB 203, § 2, 175.55(2) (“to locate an escaped prisoner”); WY HB 242 § 1, ¶ 7–3–1004(a)(iv) (“in immediate pursuit of a person law enforcement officers have reasonable suspicion or probable cause to suspect has committed an offense, not including misdemeanors . . .”). Depending on interpretation, the following additional state bills may apply to fleeing suspects: CA AB 1327 § 14350, ¶ (c) (“emergency situations”); ID SB 1134 § 1, ¶ 21–213(2) (“. . . emergency response to for safety”); MD HB 1233 § 1–203.1(B)(2)(II) (emergency exception likely to encompass fleeing suspect); and ND HB 1373 § 3, ¶ 3 (“exigent circumstances”). Eleven bills provide a carve-out to prevent the destruction of evidence and all use the same language, “to forestall (or prevent . . . the destruction of evidence.” See FL SB 92, § 1(3)(c); IL SB 1587, § 15(3); IA HF 427, § 1.3.c.; KY HB 454, § 1(3)(c); MN HF 1620/ 1706, § 3, Sub. 4(3) and MN HF 990, § 3, Subd. 4(5)(iv); ND HB 1373, § 2(c)(3)(iv) (adds the qualifier “imminent”); OH HB 207, § 4561.50(A)(3); SC H 3415, § 2. (B)(3), and WI SB 196/AB 203, § 2, 175.55(2). Only Alaska, California, Illinois, Montana, New York, and Tennessee contain explicit provisos to permit drone use where any judicially recognized exceptions to the warrant requirement would apply. AK HB 159a, amending § 2(b)(2) (“in accordance with judicially recognized exception to the warrant requirement”); CA SB No. 15, § 5, amending 14352 of PENAL CODE, ¶ (b)(“where there is an exception to the search warrant requirement”); IL SB 1587, § 30 (State may overcome presumption of inadmissibility by proving judicially recognized exception to the exclusionary rule of the Fourth Amendment . . .); MT SB 196, § 1(1)(b)(“in accordance with judicially recognized exceptions to the warrant requirement . . .”); NY AO 6244, § 1.1 (“or justified by lawful exception to the warrant requirement”); and TN SB 796, § 1(g)(2) (“absent exigent circumstances or another authorized exception to the warrant requirement” evidence obtained in violation inadmissible). 24. Bills with consent provisions include: AK HB 159a, amending § 2(b)(4) (“to monitor private land with the consent of the landowner”); AZ HB 2574, amending § 1, tit. 13, Ch. 30 ARS, 13–3007, § D.2. (“. . . enforcement . . . on public lands . . . or on private land with the written permission from the landowner”); AR HB1904, amending AR Code tit. 12, as 12–19–104(a)(1) (“operating lawfully and a person about whom information was acquired by the unmanned aerial vehicle consents to the disclosure of the information . . .”); HI SB, 263B-2(c)(1) (“. . . Consent. It shall not be unlawful under this chapter to disclose or receive information about any person acquired through the operation of an unmanned aerial vehicle if such person has given written consent to such disclosure.”); ID SB 1134, § 1.21–213(2)(a)(i)–(ii) (“. . . an individual or a dwelling owned by an individual and such dwelling’s curtilage, without such individual’s written consent; A farm, dairy, ranch or other agricultural industry without the written consent of the owner of such farm, dairy, ranch or other agricultural industry . . .”); IL SB 1586, § 15(5)(“lawful consent to search” on private property); IN SB 20, § 4(a) (“A person may not make use of an unmanned aerial vehicle without the written consent of: the person or the owner of the property or thing that is the subject of the use.”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4502.2(B) (“To collect, disclose or receive information about a person or the person’s property or area if that person has given written consent”); MA SB 1664, § 1(e) (relating to incidentally acquired information, “data collected on an individual, home, or area other than the target that justified deployment shall not be used, stored, copied, transmitted or disclosed for any purpose, except with the written consent of the data subject . . .”); MI HB 4455, § 5(a) (“. . . shall not be disclosed or received unless . . . the person has given written consent to the disclosure”); MN HF 1620/ 1706, § 2, Sub 2. (applying to private use of drones—“felony . . . if . . . without the permission of
the individual and the owner of the private property or appropriate public authority.” Consent is not mentioned regarding “agency” use of drones.; MO HB 46, § 305.637.2. (“... to conduct surveillance of any individual, property owned by an individual, farm or agricultural industry without the consent of that individual, property owner, farm or agricultural industry”); NM SB 556, § 3.A. (“... to conduct surveillance of any individual, property owned by an individual, farm or agricultural industry without the consent of that individual, property owner, farm or agricultural industry”); OK HB 1556, § 3.B.5 (“Any agency, person, organization, when acting on the informed and freely given consent of the person or organization whose person or property are the subject of the surveillance, provided the consent is made in writing prior to the commencement of surveillance”); OR HB 2710, § 4 and SB 853, § 5 (written consent); and TX HB 912, Ch. 423, § 423.002(6) (“consent of the individual who owns or lawfully occupies the real property captured in the image”). Consent would presumably be implied for state bills containing a proviso allowing drone use in accordance with judicially recognized exceptions to the warrant requirement. Massachusetts and New York bills contain provisions that permit dissemination or receipt of information only with the individual’s consent. MA SB 1664/BH 1357, § 99-C(e) (relating to incidental information collected) and NYAO 6541, § 66-A.3.(A) (relating to any person targeted).

25. Disaster response clauses can be found at: CA Assembly Bill 1327, § 14350(c)(1) and (e)(1)–(2) (law enforcement/ CAL-FIRE/other agencies can use for fires; other agencies can use for detecting oil spills); GA SB 200 § 5, ¶ (e)(2) (“to preserve public safety, protect property or conduct surveillance for the assessment and evaluation of environmental or weather related damage, erosion, flooding, or contamination during a lawfully declared state of emergency”); IA SF 276, (“during the occurrence of a disaster . . .”); ME SP 72, § 4503.2.(A), (B), (D) (natural disasters, monitor dams and flood-control systems and weather forecasting); MN HF 1620 § 3, Sub. 4, ¶ (4) (first responder may use in emergency situation) and MN HF 440, § 3, Subd.4 (6) (“during a declared state of emergency”); NJ Assembly No. 3157, ¶ 4 (“to survey or monitor the extent of a forest fire”) and NJ AB 3929, § 1.d. (“during any declared disaster or emergency to monitor, observe, photograph or record . . .”); OR HB 2710, § 5(3) and OR SB 853, § 8(1) (during a declared state of emergency to assess environmental, weather damage, erosion or contamination); TX HB 912, § 423.001(c)(3) (“fire suppression”); PA SB 85, § 5(3) and VA HB 2012, 1, § 1 (“National Guard drone exception for “purposes other than law enforcement including damage assessment . . . flood stages, and wildfire assessment”); and WV HB 2997, § 1-7-3(b) (survey environmental damage to determine if state of emergency should be declared or assess environmental, weather damage, erosion, or contamination). For SAR clauses, see CA AB 1327 § 14350, ¶ (c)(1); FL SB 92 § 1, ¶ (4)(c); ID SB 1134, § 21-213, ¶ (2); IL SB 1587, § 15(4); IA SB 276 § 12 and IA HF 410, § 2.c.; ME SP 72, § 4503.2.E.; OK HB 1556 § 3.3; OR HB 2710, § 5(1); PA SB 875, § 4; TN SB 796, § 1(d)(5); TX HB 912 § 423.002(8)(D); VA H 2012 § 1, ¶ (iv) and WI SB 196/AB 203, § 2(2). Of these, some require an imminent danger to life before a drone can be used for SAR. See, e.g., CA AB 1327 § 14350, ¶ (c)(1) (“imminent threat to life or of great bodily harm, including, but not limited to . . . search and rescue operations on land and water”); IA HF 410, § 2.c. (“during search and rescue operation if . . . necessary to protect life, health”); OK HB 1556, § 3.3.3. (“when conducting a search for a mission person, provided it is reasonable to believe that there is an imminent threat to the life or safety of the person”), PA SB 875, § 4 (“during a search and rescue operation if the deployment is necessary to protect life, health”); VA H 2012 § 1, ¶ (iv) (“for the purpose of a search and rescue operation where use of an unmanned system is determined to be necessary to alleviate an immediate danger to any person”).

315
26. IL SB 1587, § 15(5) (crime scenes); OR HB 2710, § 6(1) and OR SB 853, § 7(1) (crime scene reconstruction) and TX HB 912, § 423.002(B)-(C) (crime scene investigation and reconstruction).

27. CA AB 1327 § 14350, ¶ (d)(2) (“maximum duration not to exceed two hours”); GA HB 560, § 2(a)(4) (warrant “shall expire within 24 hours after issuance”); HI SB 783 § 1, ¶ (3)(B) (can receive a judicial order to operate drone for “no period greater than 48 hours” and within 30 days of issuance); IL SB 1587, § 15(3) (emergency operations limited to 48 hours); ME SP 72, § 4502.2. D (court order . . . “may not allow operation for a period greater than 48 hours” . . . but not to exceed 30 days); MI HB 4455 § 5(d) (court orders valid for 48 hours, with possibility of extension up to 30 days); NC HB 312 § 2(3) (“no later than 48 hours” from the date drone was used); and WA HB 1771 § 6.(4) and SB 5782, § 8(1)(c) (“Warrants shall not be issued for a [surveillance] period greater than 48 hours . . . for no longer than 30 days.”)

28. For place restrictions, see AZ HB 2574, amending § 1, tit. 13, Ch. 30 ARS, 13-3007, § B (“unlawful for a person to use drones to monitor other persons inside their homes or places of worship or within the close confines of their property or other locations where a person would have an expectation of privacy”); CA SB No. 15, § 3(j) (drone shall not be used to view “the interior of a bedroom, bathroom, changing room, fitting room, dressing room or tanning booth, or the interior of any other area in which the occupant has a reasonable expectation of privacy, with the intent to invade the privacy”); HI SB, 2563B-2(c)(3)(A)–(B) (warrants required for “non-public” areas; public areas require court orders); ID SB 1134, § 1., 21-213(2)(A)(i)(ii) (requires warrant or consent for imaging a “dwelling owned by an individual . . . dwelling’s curtilage” and “farm, dairy, ranch, or other agricultural industry”); MI HB 4455, § 3.B. (no “surveillance of an individual, or of property owned by an individual, farm or other agricultural industry” without consent); NY AO 6370/ SO 4537, § 1, S 52-A.2. (No . . . drone . . . to conduct surveillance of or to monitor any individual inside his or her home or place of worship or within the closed confines of their property or other locations where a person would have an expectation of privacy”); and ND HB 1373, § 6.4. (no surveillance “within a home or place” unless in compliance with state intercept statutes).

29. Manner restrictions with an emphasis on collecting data only on the target include: AR HB 1904, amending AR Code tit. 12, as 12-19-104(b)(1) (“in a manner to collect data only on the target and to avoid data collection on individuals, homes, or areas other than the target”); CA SB 15, tit. 14, § 14354(a) (“minimize the collection and retention of data”); HI SB, 263B-2(d) (“collect only on the target”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4502.3 (“do not collect information on a person, residence, property or area not related to a permitted purpose . . .”); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(d)(1) and (3) (“in a manner to collect data only on the warrant subject and to avoid data collection on individuals, homes, or areas other than the warrant subject”); MI HB 4455 § 5(e) (“avoid data collection on individuals, homes, or areas other than the target”); NC HB 312, § 15A-232.d ("in a manner to collect data only on the subject of the search and to avoid data collection on individuals, homes, or areas other than the subject of the search"); NY AO 6541, § 66-A.4. (“collect data only on the target and to avoid data collection in individuals, homes or areas other than the target”); OK HB 1556, § 3.F (“in a manner to collect data only on the target of the surveillance and to avoid data collection on individuals, homes, or areas other than the target”); OR HB 2710, § 1.4 (“limited to collection of information about the target person . . . and must avoid collection . . . on other persons, residences or places”) and OR SB 524, § 1(4) (limit collection to target); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3-.2.(h) (“collect data only on the designated target and shall avoid data collection on individuals, homes or areas of than the target”); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as § 4622(c)(1) (“collect data only on the target of
the surveillance and to avoid data collection on any other person, home or area”); WA HB 1771, § 4 (“conducted in such a way as to minimize the collection and disclosure of personal information not authorized under this chapter”). Some states contain unique “one off” manner restrictions or constraints. For example, GA SB 200, § 5(c) allows drones to be used only in the investigation of a felony. IL SB 1587, § 15(5) allows drone use just for crime-scene photography over public highways.

30. MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(d)(3) (“under no circumstances used . . . to collect . . . about the political, religious or social views, associations or activities of any individual, group, association or organization,” . . . etc., unless criminal investigation); ND HB 1373, § 4.3 and WV HB 2997, § 1-7-4(c) (may not use . . . “for surveillance of persons engaged in the lawful exercise of the constitutional right to freedom of speech and freedom of assembly”).

31. Biometrics is addressed in: AR HB1904, amending AR Code tit. 12, as 12-19-104(b)(3); HI SB, 2563B-2(d) (“Neither facial recognition or other biometric matching technology may be used on non-target data collected.”); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(d)(2) (“facial recognition or other biometric matching technology shall not be used on data collected . . . except to identify the subject of a warrant”); MI HB 4455 § 5(c) (“Neither facial recognition or other biometric matching technology shall be used on non-target data collected”); NC HB 312, § 15A-232.(d) (“Neither facial recognition or other biometric matching technology may be used . . . on individuals, homes or areas other than the subject of the search”); NY AO 6541, § 66-A.4 (“neither facial recognition nor other biometric matching technology shall be used on non-target data”); OR SB 853, § 4.1 (no facial recognition or biometric matching technology on non-targets); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3.-2.(h) (“Neither facial recognition or other biometric matching technology shall be used on non-target data.”); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as § 4622(c)(3) (“Facial recognition or any other biometric matching technology shall not be used on . . . other than the target . . . ”); and WA HB 1771, § 6(3) (warrants shall “not authorize the use of a biometric identification system”).

32. ME SP 72, § 4502.3 (“may not . . . employ the use of facial recognition technology”).

33. CA SB No. 15, § 5, amending PENAL CODE 14353(b) (prohibits law enforcement from receiving drone information from another agency unless they obtain warrant); CA AO 1327, § 14350(e)(3) (“no dissemination outside collecting agency”; no dissemination to LEA unless they obtain a warrant); IL SB 1587, § 25 (no disclosure except to another government agency if evidence of criminal activity or relevant to ongoing investigation or trial); MA HB 1357, § 99C(e) (no disclosure of non-target information for any purpose without written consent); WV HB 2997, § 1-7-6(c) (no distribution unless there is evidence of a crime and complies with evidentiary rules).

34. For notice to subject provisions, see HI SB, 2563B-5 (may request a delay on notification up to 90 days); ME SP 72 amends § 1, 25 MRSA Pt. 12, § 4504.3 (may request a delay on notification up to 10 days); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(g) and HB 1357, § 99C(h) (delay not to exceed 90 days; otherwise, serve notice within 7 days); MI HB 4455 § 11(1) (delay not to exceed 90 days, with possibility of 90-day extensions and delivery upon termination); OR SB 853, § 9(1) and (3) (notice to subject 10 days post-collection, can delay up to 10 days); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3.-7 (not later than 10 days after the termination of an order, the subject shall be served with information on data collected); WA HB 1771, § 6.(4) and WA SB 5782, § 6(5) (within 10 days of execution, serve a copy of warrant upon the person—may be delayed under § 7).
35. The requirement to delete information on non-targets is located in AR HB1904, amending AR Code tit. 12, as 12-19-105 (data on non-targets not to be used or disclosed and must be deleted within 24 hours after collection); HI SB, 263B-3(a) (data on non-targets not to be used or disclosed and must be deleted within 24 hours after collection); ME SP 72 amends § 1, 25 MRSA Pt. 12, § 4503 (noncompliant information must be deleted within 24 hours); MA SB 1664/MA HB 1357, § 1, amending Ch. 272 of GEN. LAWS as 99C(e) (data on non-targets not to be used or disclosed and deleted within 24 hours after collection); MI HB 4455 § 7(1) (data on non-targets not to be used or disclosed and deleted within 24 hours after collection); NY AO 6541, § 66-B (delete non-target data within 24 hours); NJ Assembly No. 3157, § 2.d. (information incidentally collected “shall be discarded”); NC HB 312, § 15A-232(g) (if collected in violation of Act, must be destroyed within 24 hours); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3.-11 (data on non-targets not to be used or disclosed and deleted within 24 hours after collection); TN SB 796, § 1(f) (non-target data to be deleted “as soon as possible” but not later than 24 hours after collection); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as § 4622(c)(2)(A)–(B) (data on non-targets not to be used or disclosed and must be deleted within 24 hours after collection); WA HB 1771/WA SB 5782, § 11 (data on non-targets not to be used or disclosed and must be deleted within 24 hours after collection); WV HB 2997, § 1-7-6(b) (evidence in violation of bill “may not be preserved”).

36. Retention limits on target information can be found in: CA Assembly Bill 1327, § 1, tit. 14, 14353(a) (“Images . . . shall be permanently destroyed within 10 days except . . . as evidence of a crime, as part of an ongoing investigation of a crime, for training purposes” or if collected pursuant to a warrant); CA SB No. 15, § 5, amending 14354 of PENAL CODE, ¶ (a) (“minimize . . . retention of data,” destroy after one year unless needed for crime investigation, “training purposes” or pursuant to a court order); IL SB 1587, § 20 (destroy within 30 days unless contains evidence of a crime, as part of an ongoing investigation, or needed for pending criminal trial); ND HB 1373, § 6.3 (90-day limit unless meets agency guidelines for evidence preservation (criminal cases); OR HB 2710, § 1.4(4) and OR SB 524, § 1(5) (“any images . . . must be destroyed within 30 days’ unless needed as evidence); TN SB 796, § 1(f) (delete target information within 24 hours); WA HB 1771/WA SB 5782, § 12 (target information, 30-day retention unless “evidence of criminal activity”); WV HB 2997, § 1-7-6(c) (90-day limitation unless there is evidence of a crime and meets evidentiary rules).

37. States with post-emergency documentation requirements include: AR HB1904, amending AR Code tit. 12, as 12-19-104(a)(2)(B) (file for warrant for emergency use of drones within 48 hours); HI SB, 263B-4(a)(4) (file for warrant or order for emergency use of drones within 48 hours); IL SB 1587, § 15(3) (law enforcement agency chief executive officer must report emergency use to state attorney within 24 hours); ME SP 72, § 4503.1.B (“not later than 48 hours after the emergency operation begins, a supervisory official for the law enforcement agency files a sworn statement setting forth the grounds for the emergency operation”); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(c)(3) (operator must document factual basis and file an affidavit not later than 48 hours later); MI HB 4455, § 5(b)(i)–(ii) (supervisory official files sworn statement containing factual basis for emergency within 48 hours after operation); MN HF 990, § 3, Subd. 5 (file detailed record of operation exercising “exception” with AG within 48 hours); NC HB 312, § 15A-232(c)(3) (supervisory official files sworn statement with clerk of the court containing factual basis for emergency within 48 hours after operation); OK HB 1556, § 3.B.3. (“reasonable articulable basis for belief . . . in a written sworn statement shall be placed in a written, sworn statement within 24 hours and . . . maintained by LEA” and by
firefighting and emergency services); OR SB 853, § 6(2) (file sworn statement with circuit court within 48 hours of emergency operation); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3-2(f)(2) (supervisory official files written statement with approval of AG to court of competent jurisdiction no later than 24 hours after operation); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as § 4623(a)(2) (requires law enforcement agency to obtain warrant within 48 hours after emergency commenced); and WA HB 1771 § 6./WA HB 5782, § 8(c) (requires warrant within 48 hours after operation begins or has occurred). Oversight and reporting requirements can be found in AR HB1904, amending AR Code tit. 12, as 12-19-106 (law enforcement agency shall file yearly reports with Legislative Council with the number of crime investigations aided by the use of drones, description of how they were helpful, number other uses and how they were helpful, frequency and type of data collected on non-targeted individuals/areas, and total cost of the program); CA AB 1327, § 14351(a) (annual reports to governor on drone purchases and details of deployments); HI SB, 263B-7 (same as AR plus reporting for judges and court administrative directors on warrants and court orders issued and denied, convictions garnered, etc.); IL SB 1587, § 35 (law enforcement agency report to criminal justice information authority annually the number of drones it owns); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4507 (same as AR, also includes provisions for AG reporting); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(i)/MA HB 1357(i) (judges report annually to court administrator on drone warrants issued or denied; court administrator to transmit compiled report to legislature annually); MI HB 4455, § 15(1)–(3) (requires operators to report biannually to legislature on public website same information as AR plus specific flight parameters; also requires extensive judiciary and AG reporting, including affidavit that no existing data violates the Act); NY AO 6541, § 66-D (annual public website reports of times used, crimes aided, collection on non-targets, and cost); NC HB 312, § 15A-232(h) (annual reporting from judiciary to Administrative Office of Courts, and then to General Assembly—law enforcement agency to which warrant was issued, offense, and nature of facilities or property searched); OR SB 71 § 4(1) (requires drone registration with state police, presumed reportable), OR SB 853, § 10 and OR 2710, § 8 (both require drone registration with OR Dep’t of Aviation and annual public reporting of use of drones by public bodies); (RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3-12 (AG reports to General Assembly annually number of times drone used, justification, number of persons upon whom information was gathered, reasons used for other than criminal, number of times collections made on non-targets, orders granted and denied, and number of resultant convictions); TX HB 912, § 423.008 (reporting every other year by law enforcement agency to governor on times used, crimes aided, collection on non-targets, and cost); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as § 4625 (law enforcement agency reports annually to Dep’t of Public Safety number of times drone used, rationale, number of investigations aided and arrests made, number of collections on non-targets, and cost of program; report to legislature; also administrative judge reports annually applications and issuance of warrants); WA HB 1771, § 15-18 and 21 and WA SB 5782, § 15-18 (extensive reporting requirements and annual “comprehensive audit” by governing body of locality; WA SB 5782 adds requirement to report on public website). For record-keeping requirements, see ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4506.4 (law enforcement agency to keep records of each operation, including all information to be otherwise reported by the AG); ND HB 1373, § 7 (all persons shall document drone flights—duration, flight path, mission objectives, etc., and retain for 5 years); WA HB 1771, § 20 (requires ordinances for law enforcement agency to maintain records of each drone use); WV HB 2997, § 1-7-7 (document all surveillance flights as to duration, flight path, mission objectives, and authorizing officials; retain for 5 years).
38. CA Assembly Bill 1327, § 1, tit. 14, 14352 ("shall provide reasonable notice to the public . . . minimum . . . a one-time announcement of . . . intent to deploy . . . and a description of technology's capabilities") and § 14352 ("images . . . shall be open to public inspection . . . unless expressly exempt by law") and CA SB No. 15, amending PENAL CODE 14354(c) ("reasonable notice to the public of acquisition" of drone); IL SB 1587, § 35 (public website listing law enforcement agencies that own drones and number they own); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4507.3 (AG annual posting to website number of applications for warrants/court orders and delays of notice granted and denied); NJ Assembly No. 3157, § 3.a. (law enforcement agency must provide public notice of purchases of UAS, including price paid, size and supplier); NY AO 6541, § 66-D (annual public website reports); NC HB 312, § 15A-232.(h) (administrative office of courts will post drone reports on its website); OR SB 853, § 10 and OR 2710, § 8 (annual public reporting of use of drones by public bodies), and WA HB 1771, §§ 19–21 ("publically (sic) available written policies and procedures" for law enforcement agencies' use of drones; audits publicly available) and WA SB 5782, §§ 15–18 (post reports on public website). See also OR SB 524, § 1(7)(a) and SB 853, § 11 (1) (must establish written training for operators, criteria for when drones will be used, description of areas in which they may be used, and procedures for informing the public on policies); VA HB 2012, § 1.1 (VA Dept. of Criminal Justice and Office of AG to develop “model protocols for use of UAS by LEA and report findings to the Governor and General Assembly” by Nov. 1, 2013).

39. CA Senate Bill No. 15, § 5, amending 14356 of PENAL CODE ("painted and labeled in a way that provides high visibility of the unmanned aircraft system"); MI HB 4455, § 3(5) (requiring drones to have the name of the owning political entity clearly printed with visible lettering on it).

40. The following bills create civil liability for drone users who violate state provisions: AZ HB 2574, amending § 1, tit. 13, Ch. 30 ARS, 13-3007, § E ("civil action against a law enforcement agency (LEA) to obtain all appropriate relief in order to prevent, restrain, or remedy a violation of this section"); CA Assembly Bill 1327, § 1, tit. 14, 14352 (personal liability) and CA SB 15, § 2, amending § 1708.8 of CIVIL CODE (creates several civil actions for actual or constructive invasion of privacy and imaging “familial activity”); FL SB 92, § 1(5) ("civil action against an LEA to obtain all appropriate relief in order to prevent, restrain or remedy a violation of this act"); ID SB 1134, § 1, 21-213(3)(a) ("civil cause of action against the person, entity or state agency"); IA HF 427, § 1.4 (civil action “to prevent or remedy”); KS HB 2394 § 1(d) ("civil cause of action" against LEA); KY HB 454, § 4 (civil action against “to obtain all appropriate relief in order to prevent or remedy”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4505 (private civil action “for legal or equitable relief” against LEA"); MD HB 1233, 1-203-1(C) (civil action against “to obtain all appropriate relief in order to prevent or remedy”); MN HF SF 1506, § 1, Sub. 4 ("civil action") and MN 1620/1706, § 3, Sub. 5 ("civil action" against an LEA “to obtain all appropriate relief in order to prevent or remedy") and MN HF 990, § 1, Subd. 6(b) (civil action against LEA or agency to recover damages, injunctive or appropriate relief); MO HB 46, § 305.641.1 and .3 ("to obtain all appropriate relief in order to prevent or remedy", "sovereign immunity is waived"); NE LB 412, § 4 ("civil action against a LEA to obtain all appropriate relief in order to prevent or remedy") and NY AO 6244, § 1. S 700.16, ¶ 3 ("may seek civil and equitable relief for a violation"); NY AO 6370/SO 4537, § 1, S 52-A.4.C. ("civil action against a LEA to obtain all appropriate relief in order to prevent, restrain, or remedy") and NY AO 6244, § 1. S 700.16, § 1, Subd. 3 ("may seek civil and equitable relief for a violation"); NJ HB 312, § 15A-232.(e) ("civil action"); ND HB 1373, § 4 ("civil action to obtain all appropriate relief to prevent or remedy"); OH HB 207, § 4561.50(C) (civil action for damages); OK HB 1556, § 3.D. ("civil action against responsible party"); OR
HB 2710, § 14–15 (liability for taking control of FAA-licensed or U.S. Armed Forces-operated drone; liability for flying less than 400 feet over private property), OR SB 71, §§ 5–6 (strict liability for injuries caused by drone operation; liability for gaining unauthorized control over a drone); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3.-10. (civil cause of action); SC H 3415, § 2(C) (civil action to prevent or remedy); TN HB 591, § 1(e) (civil action “to obtain all appropriate relief in order to prevent or remedy a violation”); TX HB 912, Ch. 423, § 423.006(2)–(3) (civil action to recover civil penalties); WA HB 1771, § 13 (“legal action for damages”); WV HB 2732, Art. 7, § 1-7-5. (“civil action against LEA to obtain all appropriate relief in order to prevent or remedy a violation”) and WV HB 2997, § 1-7-5 (“all appropriate relief to prevent or remedy”).

41. Injunctive relief provisions include: AL SB 317, § 1(c) (“civil action . . . to prevent”); AZ HB 2574, amending § 1, tit. 13, Ch. 30 ARS, 13-3007, § E (“civil action against a law enforcement agency to obtain all appropriate relief in order to prevent”); CA Assembly Bill 1327, § 1, tit. 14, 14352 (personal liability . . . person imaged without consent may seek “injunction prohibiting use of images . . .”) and CA SB No. 15, § 2(h) (“an injunction and restraining order”); FL SB 92, § 1(S) (“civil action against a LEA to obtain all appropriate relief in order to prevent, restrain or remedy a violation of this act”); IA HF 427, § 1.4 (civil action “to prevent or remedy”); KS HB 2394 § 1(d) (equitable relief); KY HB 454, § 4 (civil action against “to obtain all appropriate relief in order to prevent or remedy”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4506 (private or AG-initiated civil action “for legal or equitable relief”); MD HB 1233, 1-203-1(C) (civil action against “to obtain all appropriate relief in order to prevent or remedy”); MN 1620/ 1706, § 3, Sub. 5 (“civil action” against an LEA “to obtain all appropriate relief in order to prevent or remedy”); MO HB 46, § 305.641.1 (“to obtain all appropriate relief in order to prevent or remedy”); NM SB 556, § 5.A. (civil action “to obtain all appropriate relief in order to prevent or remedy a violation”); ND HB 1373, § 4 (“civil action to obtain all appropriate relief to prevent or remedy”); OK HB 1556, § 3.D. (“shall be liable for treble actual damages” and for willful or wanton conduct or deliberate efforts to conceal violations, “punitive damages not to exceed $50,000”); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3.-10 (actual damages but not less than liquidated damages of $100 per day of violation or $1,000, whichever is higher; punitive damages and reasonable attorney’s fees; good-faith reliance on order is a defense); TX HB 912, Ch. 423, § 423.005(b)–(d) ($1,000 for each image—subject to adjustment of the amount—court costs and
reasonable attorney’s fees); WA HB 1771, § 13 (actual damages, mental pain and suffering, or liquidated damages at $1,000 per day for each day of violation not to exceed $10,000, reasonable attorney’s fees, and costs of litigation). See provisions outlined in note 91 for further details.

43. Criminal liability is found in: AK HB 159a, § 2(d) (“unlawful use of an unmanned aerial vehicle is a class A misdemeanor”); AZ HB 2574, amending § 1, tit. 13, Ch. 30 ARS, 13-3007, § F. (“Class 6 felony”); CA SB No. 15, § 3(j) (disorderly conduct misdemeanor for using unmanned aircraft system to view “the interior of a bedroom, bathroom, changing room, fitting room, dressing room or tanning booth, or the interior of any other area in which the occupant has a reasonable expectation of privacy, with the intent to invade the privacy; view identifiable person under or through their clothing for the purpose of viewing the body or undergarments of . . .; or viewing anyone in a state of full or partial undress,” § 5(b) criminalizes use of a weaponized drone); GA HB 560, § 2(b)–(d) (any LEA of the U.S. or Georgia who uses a drone without a warrant, or assists them, “shall be guilty of a misdemeanor”); IN SB 20, § 4(b) (knowing or intentional use of drone in violation is “Class D felony”); MI HB 4455, § 17 (flying an armed drone is a felony punishable by no more than 10 years imprisonment or a fine between $1,000 to $10,000 or both; other violations are a misdemeanor of not more than a year imprisonment and fine between $500 and $5,000; also criminalizes intentional disclosure and “significant reporting errors” as separate misdemeanors); MN 1620/1706, § 3, Subd.2 (felony if private person uses a drone to capture images on public or private property without permission . . .), MN HF 990, § 1, Subd. 6(a) (gross misdemeanor for violating documentation requirements); MT SB 196, § 1(1)(c) (UAV collection offense—fined not more than $500, incarcerated not longer than 6 months, or both); NH HB 619, IV.-a. (Class A misdemeanor for knowingly creating or assisting in creating an image of the exterior of any residential dwelling by or with the assistance of a drone . . . but not applicable to LEA); NJ Assembly No. 3157, § 5 (criminalizes private purchase, ownership or possession of a drone as a “disorderly persons offense” and a fine of up to $10,000, up to 18 months imprisonment, or both—not applicable to LEA, Forest Service, or U.S. military member on duty traveling to or from an authorized place of duty); NM SB 556, § 5.C. (petty misdemeanor); NY AO 6370/SO 4537, § 1, S 52-A.4.A. (Class B misdemeanor unless used in the commission of a felony, then Class C felony); NC HB 312, § 15A-232.(c) (if used for gathering evidence, Class 1 misdemeanor; if violates data retention rules, Class 3 misdemeanor); OK HB 1556, § 4.D. and 5.B. (willful disclosure . . . misdemeanor not to exceed 6 months in the county jail and a fine between $250 and $2,500 per violation; felony to operate weaponized drone—10 years and between $1,000 and $10,000 for each violation—not applicable to military “over public land for purposes of testing or training”); OR HB 2710, § 13(1) (Class A felony to intentionally fire a bullet/projectile, direct a laser or crash into an aircraft in the air, or gain authorized control over an FAA-licensed or U.S. Armed Forces–operated drone) and OR SB 71, §§ 2–3 (contains laundry list of misdemeanors and felonies, similar to OR HB 2710 and adds “to hunt or stalk game”); TX HB 912, Ch. 423, § 423.004 (illegal use, possession, disclosure, display, distribution, or use of image all Class C misdemeanors; each image is a separate offense); WA SB 5782, § 13 (Class C felony to disclose personal information without court authorization); WI SB 196/AB 203, § 3, amending § 941.292 of the statutes (Class H felony to sell transport, manufacture, possess, or operate weaponized drone; collection on person with “reasonable expectation of privacy” is a Class A misdemeanor).

44. Administrative disciplinary provisions can be found in HI SB, 263B-3(c) and 263B-6 (“administrative discipline” for willful disclosure or use of information beyond that permitted); MI HB 4455, § 13(1) (willful or intentional violations require determination, and notification to AG, as to whether or not “disciplinary action” will occur; in cases of negligence, AG may have to
approve operator/agency’s use of drone per § 13(2)); NY AO 6541, § 66-C.1. (for willful violations).

45. See Appendix B for the list of federal drone bills. Several of these federal bills discuss use of drones for targeted killings overseas, focus on “civil unmanned aircraft systems” in the United States, or discuss the requirement for drones for border patrol in the context of immigration. See HR 2438, Designating Requirement on Notification of Executive-Ordered Strikes Act of 2013 (DRONES Act) (R. Darrell Issa, R-CA), http://www.gpo.gov/fdsys/pkg/BILLS-113hr2438ih/pdf/BILLS-113hr2438ih.pdf and HR 2183, Drones Accountability Act (R. Barbara Lee, D-CA), http://www.gpo.gov/fdsys/pkg/BILLS-113hr2183ih/pdf/BILLS-113hr2183ih.pdf; The latter forbids the military to execute strikes for the Central Intelligence Agency. § 1057, the Safeguarding Privacy and Fostering Aerospace Innovation Act of 2013 focuses on private users. It prohibits private drone users from “willfully” conducting surveillance on another person, unless given prior written consent, in an emergency situation or in a public location “where surveillance would not be highly offensive to a reasonable person.” The remedies for violation include a civil action and fines. It also requires marking of civil drones with the name, address, and telephone number of the owner. Use of drones for border security is included in HR 830, Secure America through Verification and Enforcement Act of 2013 (SAVE Act), and HR 2124, Keeping the Promise of ICRA Act, http://www.gpo.gov/fdsys/pkg/BILLS-113hr830ih/pdf/BILLS-113hr830ih.pdf.

46. HR 972, Preserving Freedom from Unwarranted Surveillance Act of 2013, or PAPA.

47. Id. § 2, warrant exception; § 3(2) for a danger to life, property, and fleeing-felon exception found in many states. Also, like most states, HR 972, § 3(3) defines the terrorist attack exception as “use of a drone to counter a high risk of a terrorist attack by a specific individual or organization, when the Secretary of Homeland Security determines credible intelligence indicates there is such a risk.”

48. Id. § 4.

49. HR 1262, Drone Aircraft Privacy and Transparency Act of 2013; HR 2868, Drone Aircraft Privacy and Transparency Act of 2013. The only difference between these two bills is that HR 1262 contains a “Findings” section that HR 2868 does not.

50. HR 1262, § 341; HR 2868, § 3(a)(1).

51. HR 1262 and HR 2868, § 341(a)–(b).

52. Id. § 341(b)(3)–(4).

53. Id. §§ 337–339. The data minimization statement would include certification that non-target data and target data that is no longer relevant to investigation of a crime under a warrant or to an ongoing criminal proceeding will be redacted. See id. § 339(c)(1)(B).

54. Id. § 340.

55. HR 1262, § 4(c); HR 2868, § 3(c)(1). For private causes of action, remedies include injunction, damages up to $1,000 a day for each violation or both, and for intentional violations, treble damages. Recovery of attorney’s fees and court costs is also possible.

56. HR 1262 and HR 2868, § 341(b)(6).

57. HR 1262, § 4(a)–(b); HR 2868, § 3(B)(1).

58. HR 1262, § 4(f); HR 2868, § 3(f).

59. H.R. 637, Preserving American Privacy Act of 2013 (PAPA). As do some states, the PAPA also addresses private, or nongovernmental, use of drones. Like CA SB No. 15, it makes it unlawful to intentionally collect, “in a manner highly offensive to a reasonable person,” images of individuals “engaging in a personal or familial activity under circumstances in which the individual had a reasonable expectation of privacy. Unlike the California bill, the PAPA fails to describe the remedy for such a violation.” Id. § 3119f.; CA SB No. 15.

60. Id. § 3119a(2)(A)–(B).
Intersection of Domestic Counterterrorism Operations and Drone Legislation

61. *Id.* Ch. 205A, § 3119c(c)(b)(1)–(5).

62. *Id.* § 3119c(5)(B).

63. *Id.* § 3119c(2)(B)–(D).

64. *Id.* § 3119c(1)(B).

65. *Id.* § 3119e.

66. *Id.* § 3119b(b) and (c). The data collection statement would include the purpose of the operation, whether the drone is capable of collecting covered information, data retention time, a point of contact for citizen feedback, the responsible unit, the rank and title of the person authorizing the operation, data minimization policies, as well as oversight procedures. Like the DAPTA’s, information relevant to the investigation of a crime may be retained. HR 637, § 3119b(c)(1)(A)–(H). This is similar to information required in a DoD Proper Use Memorandum (PUM). See, e.g., AFI 14-104, Attachment 4.

67. *Id.* § 3119d(a)

68. *Id.* § 3119i.

69. 18 U.S.C. § 1385. The PCA does not apply to National Guard forces in title 32, U.S. Code, or state active duty status, and they are thus able to more readily assist law enforcement.


72. DoDI 3025.21, Encl. 3, § 5(a)–(b). See also DoDD 3025.18, ¶ 4o; DepSecDef Memo, Sept. 28, 2006; DoDI 3025.22, *The Use of the National Guard for Defense Support of Civil Authorities*, July 26, 2013, http://www.dtic.mil/whs/directives/corres/pdf/302522p.pdf. DoD Instructions implement DoD Directives. Requests for SecDef approval for domestic use of drones are forwarded to the CJCS through the military chain of command. The approval package includes sufficient information on the activity or event to allow deciding officials to make an informed judgment on its propriety, a Proper Use Memorandum (PUM), and an FAA Certificate of Authorization (CoA) or license. PUMs are required by regulation and signed by an officer in a position of authority, normally after legal review, who certifies the legitimacy of proposed domestic imagery requirements and the appropriateness of use parameters as well as legal and policy compliance. AFI 14-104, ¶ 9.5, Attachment 1 Terms and Attachment 4. For a detailed review of approval authorities for DoD domestic imagery missions, see Dawn M.K. Zoldi, Colonel, USAF, *Protecting Security and Privacy: An Analytical Framework for Airborne Domestic Imagery*, pending publication in *Air Force L. Rev.*, Vol. 70, 2013 Ed.
Colonel Dawn M.K. Zoldi

73. 2013 Chairman Joint Chiefs of Staff Defense Support of Civil Authorities Execute Order (CJCS DSCA EXORD), 071415z Jun 13, ¶ 3.C.4.J.1. An EXORD is “[a]n order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to implement a decision by the President to initiate military operations.” JP 1-02, p.97.

74. Id. at ¶ 1.J.

75. The term “Incident Awareness and Assessment” (IAA) is defined as “The Secretary of Defense approved use of Department of Defense intelligence, surveillance, reconnaissance, and other intelligence capabilities for domestic non-intelligence support for defense support of civil authorities.” JP 1-02, p.131.

76. CJCS DSCA EXORD 2013, ¶ 3.C.4.J.1. If a drone or other intelligence capability is used for these DSCA missions, they must be conducted in accordance with the intelligence oversight (IO) requirements, discussed below.


78. DoDI 3025.21, Enc. 3, ¶ 1c(1)(a)–(g).

79. DoDI 3025.21, Enc. 6.


81. 10 U.S.C. § 374(b)(1)(C) and (b)(2)(C).

82. JP 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, p. 231.

83. Drones are an intelligence, surveillance, and reconnaissance (ISR) platform and, as such, are considered an intelligence capability. ISR refers “to an activity that synchronizes and integrates the planning and operation of sensors, assets and processing, exploitation and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.” DoD Directive 5143.01, Under Secretary of Defense for Intelligence (USD(I)), Nov. 23, 2005, ¶ E2.1.7 (citing to JP 1-02). That said, there is no doctrinal document that authoritatively states that drones should, in all circumstances, be considered an “intelligence capability.” Some have suggested the RPA’s categorization depends on the activity or mission it is conducting at any given moment. Dawn M.K. Zoldi, Colonel, USAF, Protecting Security and Privacy: An Analytical Framework for Airborne Domestic Imagery, pending publication in THE AIR FORCE L. REV., Vol. 70, 2013. However, the SecDef routinely directs that during DSCA missions, Intelligence Oversight (IO) rules will apply. See also 2013 CJCS DSCA EXORD.


85. DoD 5240.1-R defines counterintelligence as “[i]nformation gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or international terrorist activities, including personnel, physical, document or communications security programs.” Id. at DL1.1.5. Foreign intelligence is defined as “[i]nformation relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on intentional terrorist activities.” Id. at DL1.1.11.

86. E.O. 12,333, ¶ 2.3; DoD 5240.1-R, ¶ C2.3. Again, drones do not actually collect. Their sensor operators do.

87. DoD 5240.1-R, ¶ C2.4.2. Collection rules are contained in Procedure 2 of DoD 5240.1–R. DoD 5240–1R defines a USPER at DL1.1.25 as a U.S. citizen; an alien known to be a permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; a corporation incorporated in the U.S. exception for those directed and controlled by a foreign government. A person located in the U.S. is presumed to be a USPER.

88. Id. ¶ C2.4.1

89. Id. ¶ C2.4.2–2.4.2.4.

90. For example, in non-emergent situations, electronic surveillance, referred to as a Procedure 5, may only be conducted pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. § 36. Only the SecDef, DepSecDef, the Secretary of the Air Force (SecAF), or the Director of the National Security Agency (NSA) can submit a request for a FISA warrant for this purpose. DoD 5240.1-R, ¶ C5.1.2. See also: Procedure 6—Concealed Monitoring, ¶ C.6.3.3.; Procedure 7—Non-Consensual Physical Searches, ¶ 7.3.2; Procedure 8—Mail Searches and Examination, ¶ 8.3; Procedure 9—Physical Surveillance, ¶ 9.3.3; Procedure 10—Undisclosed Participation in Organizations, ¶ 10.3.2.

91. DoD 5240.1-R, C.12.2.2.3, and 12.2.2.3.4.

92. DoDI 3025.21, Encl. 3.


95. DoD 5240–1.R, ¶ C3.3.4.

96. Id. ¶ C3.3.2.4. Other exceptions for retaining USPER data are outlined in Procedure 3.

97. Id. ¶ C4.2., also called “Procedure 4.”

98. Id. ¶ C4.3.

100. The following drone bills contain weapons restrictions: AR HB 1904 § 12-19-104, ¶ (d) (“An unmanned aerial vehicle shall not be equipped with weapons.”); CA SB No. 15, § 5, amending tit. 14, § 14350 of the PENAL CODE, § 14351(a) (“may not be equipped with a weapon”) and CA AB 1327, § 14354.5 (not equip or arm an unmanned aircraft system with a weapon or other device that may be carried or launched . . .); GA SB 200 § 3, ¶ (1) (prohibits equipping an unmanned aircraft with weaponry); HI SB 783 § 1, ¶ (e) (“unmanned aerial vehicles may not be equipped with weapons”); IA SB 276 § 14 (“under no circumstances shall a weaponized unmanned aircraft system be deployed”), IA HF 410, § 1.3. (“under no circumstances shall a weaponized unmanned aircraft system be deployed . . . by the state . . .”); KS HB 2394 § 1, ¶ (b) (“no drone shall be operated in this state while carrying a lethal payload”); KY 14 RS BR 1, § 1(2) (“no prohibited agency shall use a drone carrying a lethal payload”); ME SP 72 § 4502.3 (“An unmanned aerial vehicle may not be equipped with a weapon.”); MA SB 1664 § 1, ¶ (b) and MA HB 1357, § 99-C(b) (“Unmanned aerial vehicles may not be equipped with weapons.”); MI HB 4455 § 3, ¶ (4) (“shall not operate UAV that contains, mounts, or carries a lethal or nonlethal weapon or weapon system of any type”); MN HF 990, § 3, Subd. 3 (no drones equipped with dangerous weapons or nonlethal devices); ND HB 1373 § 4, ¶ 1 (“A state agency may not authorize the use, including grant a permit to use, of an unmanned aircraft while armed with any lethal or nonlethal weapons.”); NY AO 6541 § 66-A.5. (no lethal or nonlethal weapons); OK HB 1556, § 5.A (“contains, mounts, or possesses any lethal or nonlethal weapon”); OR HB 2710, § 10 (“A public body may not operate a drone that is capable of firing a bullet or other projectile, directing a laser or otherwise being used as a weapon”) and OR SB 524, § 1(6)(“may not use a drone that is capable of firing a bullet or other projectile”); PA SB 875, § 5 (“a weaponized unmanned aircraft system may not be deployed or its use facilitated by a State or local agency or member of the public.” Exempts National Guard); SC GA Bill 395, Ch. 39, § 6-39-20 (“may not own, use, contract for or otherwise obtain services from a drone containing an antipersonnel device”); VT H 540, § 4622, ¶ (e) (“Drones shall not be equipped with weapons.”); VA HB 2012 § 1, ¶ 1 (“In no case may a weaponized unmanned aircraft system be deployed.”); WV HB 2732 § 1-7-3, ¶ (b) (“No drone operated within the State of West Virginia may carry a lethal payload.”) and WV HB 2997, § 1-7-4(b) (may not authorize use of unmanned aircraft while “armed with any lethal or non-lethal weapons, including firearms, pepper spray, bean bag guns, mace and sound-based weapons”); and WI SB 196/AB 203, § 3 (“sale, transport, manufacture, possession or operation of weaponized drone is Class C felony”).

101. CA AB 1327, § 14354.5 (“may not equip or arm an unmanned aircraft system with . . . device that may be carried or launched . . .”); MI HB 4455 § 3, ¶(4) (“shall not operate UAV that contains, mounts, or carries a . . . nonlethal weapon or weapon system of any type”); MN HF 990, § 3, Subd. 3 (no drones equipped with . . . non-lethal devices); ND HB 1373 § 4, ¶ 1 (“A state agency may not authorize the use, including grant a permit to use, of an unmanned aircraft while armed with any . . . nonlethal weapons.”); NY AO 6541 § 66-A.5. (no nonlethal weapons); OK HB 1556, § 5.A (“contains, mounts, or possesses any lethal or nonlethal weapon”); OR HB 2710, § 10 (“A public body may not operate a drone that is capable of firing a . . . projectile, directing a laser or otherwise being used as a weapon”) and OR SB 524, § 1(6)(“may not use a drone that is capable of firing . . . projectile”); WV HB 2997, § 1-7-4(b) (may not authorize use of unmanned aircraft while “armed with any . . . non-lethal weapons, including firearms, pepper spray, bean bag guns, mace and sound-based weapons”).

102. WV HB 2997, § 1-7-4(b).

103. OR HB 2710, § 10.

104. States with criminal exclusionary rules include AL SB 317, § 1(d) (“criminal prosecution”); AK HB 159a, § 3(a) (“criminal action or proceeding”); AZ HB 2574, amending
Intersection of Domestic Counterterrorism Operations and Drone Legislation

§ 1, tit. 13, Ch. 30 ARS, 13-3007, § C (“collected or obtained in violation . . . not admissible in any . . . criminal proceeding”); AR HB1904, amending AR CODE tit. 12, as 12-19-105(b) (limited to non-targets; “information acquired and evidence derived from its use shall not be received in evidence in any trial, hearing or other proceeding”); FL SB 92, § 1(5) (“not admissible as evidence in a criminal prosecution in any court of law in this state”); GA HB 560, § 2(e) (“inadmissible in any . . . proceeding”); HI SB, 2563B-3(b) (“in any trial”); IL SB 1587, § 30 (compliance a prerequisite for admissibility “but nothing in this Act shall prevent a court from independently reviewing the admissibility of evidence for compliance with the Fourth Amendment to the U.S. Constitution or with Article I, Section 6 of the Illinois Constitution”); IN SB 20, § (5) (“not admissible as evidence in an administrative or judicial proceeding”); IA HF 427, § 1.5 (“not admissible in criminal trial”); KS HB 2394 § 1(e) (“in any trial, hearing or other proceeding”); KY HB 454, § 5 (in any criminal proceeding . . . for the purpose of enforcing state or local laws”) and KY 14 RS BR 1, § 1(5) (“not admissible as evidence in any civil, criminal or administrative proceeding . . . to enforce state or local law”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4503 (compliance required for admissibility in “trial, hearing or other proceeding”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4506.3. (“a court . . . shall grant a motion to suppress as evidence”); MD HB 1233, 1-203-1(D) (“not admissible as evidence in a criminal prosecution”); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(f) and MA HB 1357, § 99-C(f) (“any judicial, regulatory or other government proceeding”); MI HB 4455 § 7(2) (“information acquired will not be admitted into evidence in a trial, hearing or other proceeding”); MN HF SF 1506, § 1, Sub. 5 (criminal prosecution), MN 1620/1706, § 3, Sub. 5 (“not admissible as evidence in a criminal prosecution”); MN HF 990, § 1, Subd. 7 (“in a civil action or criminal prosecution in this state”); MO HB 46, § 305.641.2 (“as evidence in a criminal proceeding . . .”); MT SB 196, § 1(1)(b) (“not admissible in any proceeding . . . may not be used for any purpose”); NE LB 412, § 6 (“not admissible as evidence in a criminal prosecution”); NJ Assembly No. 3157, § 2.d (incidentally collected information shall not “be used as evidence in court for a crime” unrelated to an investigation of the target) and NJ AB 3929, ¶ 3 (“as evidence in a criminal prosecution”); NM SB 556, § 5.B. (“evidence in criminal proceeding in any court”); NY AO 6370/SO 4537, § 1, § 52-A.4.B. (criminal proceeding in any court), NY AO 6244, § 1, § 700.16, ¶ 3 (“inadmissible in any criminal action”); NY AO 6541, § 66-B.2 (“in any trial, hearing or other proceeding”); NC HB 312, § 15A-232.(f) (“criminal, civil or administrative proceeding”); ND HB 1373, § 6.1 (“criminal prosecution or administrative hearing”—but exclusion does not apply to incidentally acquired information); OH HB 207, § 4561.50(B) (“trial, hearing or other proceeding”); OK HB 1556, § 3.E. and § 4.E. (“No information, data, media . . . shall be received in evidence in any trial, hearing or other proceeding.”); OR HF 2710, § 11 (if drone has not been approved by FAA, evidence inadmissible in judicial and administrative proceedings), OR SB 71, § 4(3) (obtained in violation of act, not admissible in any judicial or administrative proceeding), and OR SB 853, § 4(2)(a) and 8(2)(a) (non-target data inadmissible in any judicial or administrative proceeding; surveillance during state of emergency not admissible); RI Gen. Assembly Jan. 2013, amending tit. 12 of GEN. LAWS, Ch. 5.3, 12-5.3.-8., 9, and 11. (exclusion of evidence and derivative evidence if person not served notice of information collected not 10 days prior to proceeding and very detailed parameters for suppression of evidence based on unlawfully obtaining information, facial insufficiency of order, drone use not in conformity with the order or notice/service not made pursuant to the Act; also exclusion for violating retention rules) and RI LC00564, § 12-5.3.2 (information gathered without a warrant, or derived therefrom, not admissible in any civil or criminal court); SC H 3415, § 2(D) (“not admissible as evidence in a criminal prosecution”); TN HB 591, § 1(f) (“shall not be admissible as evidence in a criminal prosecution”) and TN SB 796, § 1(g)(2) (evidence obtained in violation not admissible as evidence
in criminal prosecution); TX HB 912, Ch. 423, § 423.005(1) (“may not be used as evidence in any criminal or juvenile proceeding, civil action or administrative proceeding”—except to prove a violation of the Act); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as § 4622(d) (“inadmissible in any judicial or administrative proceeding”); WA HB 1771/WA SB 5782, § 10 (blanket exclusion on admissibility of any personal information acquired from a drone); WI SB 196/AB 203, § 5, amending § 972.113 (in violation, no admissible in criminal proceeding); WV HB 2732, Art. 7, § 1-7-6 (“not admissible as evidence in a criminal prosecution”) and WV HB 2997, § 1-7-6(a) (in violation not admissible in criminal or administrative hearings); WY HB 0242, 7-3-1005 (“in any criminal proceeding”). Even if the state fails to include a specific criminal exclusionary provision in its drone bill, it is safe to assume that the courts in those states that require a warrant would still exclude the evidence consistent with their constitution or other law if law enforcement did not obtain a warrant, unless a judicial exception to the warrant requirement applied.

105. For civil or administrative exclusionary rules see: AK HB 159a, § 1(a) (“civil action or proceeding”); AZ HB 2574, amending § 1, tit. 13, Ch. 30 ARS, 13-3007, § C (“collected or obtained in violation . . . not admissible in any . . . civil proceeding”); AR HB1904, amending AR CODE tit. 12 as 12-19-105(b) (limited to non-targets only—“information acquired and evidence derived from its use shall not be received in evidence in any trial, hearing or other proceeding”); GA HB 560, § 2(e) (inadmissible in any civil . . . proceeding”); HI SB, 2563B-3(b) (“in any trial”); IL SB 1587, § 30 (compliance a prerequisite for admissibility, “but nothing in this Act shall prevent a court from independently reviewing the admissibility of evidence for compliance with the Fourth Amendment to the U.S. Constitution or with Article I, Section 6 of the Illinois Constitution”); IN SB 20, §(5) (“not admissible as evidence in an administrative or judicial proceeding”); KS HB 2394 § 1(e) (“in any trial, hearing or other proceeding”); KY HB 454, § 5 (in any civil . . . or administrative proceeding . . . “for the purpose of enforcing state or local laws”) and KY 14 RS BR 1, § 1(5) (“not admissible as evidence in any civil, criminal or administrative proceeding . . . to enforce state or local law”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4503 (compliance required for admissibility in “trial, hearing or other proceeding”); ME SP 72, amends § 1, 25 MRSA Pt. 12, § 4506.3. (“a court . . . shall grant a motion to suppress as evidence”); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(f) (“any judicial, regulatory or other government proceeding”) and MA HB 1357, § 99-C(f) (“any judicial, regulatory or other government proceeding”); MI HB 4455 § 7(2) (“information acquired will not be admitted into evidence in a trial, hearing or other proceeding”); MN HF 990, § 1, Subd. 7 (“in a civil action or criminal prosecution in this state”); MO HB 46, § 305.641.2 (“as evidence in . . . an administrative hearing”); MT SB 196, § 1(1)(b) (“not admissible in any proceeding . . . may not be used for any purpose”); MT SB 196, § 2(3) (“not admissible as evidence in any prosecution or proceeding”); NM SB 556, § 5.B (“evidence in administrative hearing”); NY AO 6370/SO 4537, § 1, S 52-A.4.B (“civil proceeding in any court . . . or in an administrative hearing”); NY AOS 6541, § 66-B.2 (“in any trial, hearing or other proceeding”); NC HB 312, § 15A-232(f) (“criminal, civil or administrative proceeding”); OH HB 207, § 4561.50(B) (“trial, hearing or other proceeding”); OK HB 1556, § 3.E & 4.E (“No information, data, media . . . shall be received in evidence in any trial, hearing or other proceeding . . . except for that introduced in any proceeding brought against a violator of this act.”); OR HF 2710, § 11 (if drone has not been approved by FAA, evidence inadmissible in judicial and administrative proceedings), OR SB 71, § 4(3) (obtained in violation of act, not admissible in any judicial or administrative proceeding), and OR SB 853, §§ 2(1), 4(2)(a) 8(2)(a) (collected in violation/derived therefrom not admissible; non-target data inadmissible in any judicial or administrative proceeding; surveillance during state of emergency not admissible); RI LC00564, § 12-5.3-2 (without a warrant, inadmissible in any
Civil or criminal court); TX HB 912, Ch. 423, § 423.004 (“may not be used as evidence in any criminal or juvenile proceeding, civil action or administrative proceeding”—except to prove a violation of the Act); VT HB 540/SB 16, amending § 1 20 V.S.A. Ch. 205 as § 4622(d) (“inadmissible in any judicial or administrative proceeding”); WA HB 1771/WA SB 5782 § 10 (blanket exclusion on admissibility of any personal information acquired from a drone) and WV HB 2997, § 1-7-6(a) (in violation not admissible in criminal or administrative hearings).

106. Derivative evidence exclusions include AR HB1904, amending AR CODE tit. 12 as 12-19-105(b) (limited to non-targets; “information acquired and evidence derived from its use shall not be received in evidence in any trial, hearing or proceeding”); GA HB 560, § 2(e) (information “gathered as a result . . . of drone use without a warrant is inadmissible”); HI SB, 2563B-3(b) (“no evidence derived therefrom”); IN SB 20, § (5) (“evidence derived from a communication or image”); KS HB 2394 § 1(e) (“evidence derived therefrom”); MA SB 1664, § 1, amending Ch. 272 of GEN. LAWS as 99C(f) (“and information derived therefrom”); MI HB 4455 § 7(2) (“and evidence derived from the operation”); NJ Assembly No. 3157, § 2.d (incidentally collected information shall not “be used as evidence in court for a crime” unrelated to an investigation of the target); NY AO 6370/SO 4537, § 1, S 52-A.4.B (“and all evidence derived from such evidence or information”); OH HB 207, § 4561.50(B) (“no information collected . . . and no evidence derived therefrom”); OK HB 1556, § 3.E & 4.E (“and no evidence derived therefrom”); OR HF 2710, § 11 (if drone has not been approved by FAA, no information collected or evidence derived from that image), OR SB 853, § 2(1) and 4(2)(a) (collected in violation/derived therefrom not admissible; non-target data and information derived therefrom inadmissible); RI LC000564, § 12-5.3-2 (without a warrant, evidence and information derived therefrom inadmissible in any civil or criminal court); WA HB 1771/WA SB 5782 § 10 (blanket exclusion on admissibility of any personal information acquired from a drone and “no evidence derived therefrom”).

107. MT SB 196, § 2(3, “Information obtained from the operation of an UAV . . . may not be used in an affidavit of probable cause in an effort to obtain a search warrant (unless obtained in compliance with the Act).”); OR HF 2710, § 11(2) (if drone has not been approved by FAA, no information collected or evidence derived from that image), OR SB 853, § 2(1) and 4(2)(a) (collected in violation/derived therefrom not admissible; non-target data and information derived therefrom inadmissible); RI LC000564, § 12-5.3-2 (without a warrant, evidence and information derived therefrom inadmissible in any civil or criminal court); WA HB 1771/WA SB 5782 § 10 (blanket exclusion on admissibility of any personal information acquired from a drone and “no evidence derived therefrom”).

108. H.R. 1083, The No Armed Drones Act of 2013 (NADA). Person is defined at 49 U.S.C. § 40102(a)(37) as including “a governmental authority and a trustee, receiver, assignee, and other similar representative.” It is beyond the scope of this chapter to discuss whether the SecTrans can preclude the President of the United States (POTUS) from operating a weaponized drone under his Article II authority.

109. H.R. 637, § 3119h.

110. H.R. 1269, Life, Liberty, and Justice for All Americans Act (Rep. Trey Radel, R-FL), available at http://www.gpo.gov/fdsys/pkg/BILLS-113hr1269ih/pdf/BILLS-113hr1269ih.pdf. The bill defines “lethal military force” as meaning “a targeted killing or other lethal action . . . that is typically used against an enemy of the United States.”

111. S. 505, Bill to prohibit use of drones to kill US citizens in U.S. (Sen. Ted Cruz, R-TX), available at http://www.gpo.gov/fdsys/pkg/BILLS-113s505pcs/pdf/BILLS-113s505pcs.pdf. Again, whether or not Congress can limit POTUS’s Article II powers is a matter beyond the scope of this chapter.

 Colonel Dawn M.K. Zoldi


114. H.R. 1262, § 341(b)(6); H.R. 2868, § 341(b)(5).

115. H.R. 637, Ch. 205A, § 3119c(c)(a).

116. DoDD 3025.18, ¶ 4.o.

117. Att’y Gen. Holder, Letter to Senator Paul, March 7, 2013, note 113, supra. Note that in a previous memo to Sen. Paul dated March 4, Holder had stated it was “possible . . . to imagine an extraordinary circumstance in which it would be necessary and appropriate under the Constitution and applicable laws of the United States for the President to authorize the military to use lethal force within the territory of the United States.” The example he gave for this was “to protect the homeland in circumstances of a catastrophic attack like the ones suffered on December 7, 1941, and September 11, 2001.” See note 2, supra. Jack Goldsmith, of the Brookings Institute, wrote an excellent exposition of the many legal bases for a President to actually, under some circumstances, lawfully order lethal force against an American on American soil, including Article II of the Constitution and the Insurrection Act. See http://www.lawfareblog.com/2013/02/of-course-president-obama-has-authority-under-some-circumstances-to-order-lethal-force-against-a-u-s-citizen-on-u-s-soil-and-a-free-draft-resposne-to-senator-paul-for-john-brennan/.

118. State exclusionary provisions, however, could impact the use of DoD-collected information in state court. For example, in the Air Force, intelligence components must report to the appropriate civilian law enforcement agencies any incidentally acquired information reasonably believed to be a violation of law or relating to potential threats to life or property (whether DoD personnel, installations, or activities, or civilian lives or property). AFI 14-104, ¶¶ 11.12.1, 11.12.2.2, and 12; 10 U.S.C. § 371, Use of information collected during military operations, http://www.law.cornell.edu/uscode/text/10/371. However, some states, like Michigan, prohibit their local law enforcement agencies from receiving information or evidence acquired by a drone and if they do so, preclude its admissibility in court. MI HB 4455, § 3(3): “Except as provided in section 5, a law enforcement agency of this state or a political subdivision of this state shall not disclose or receive information acquired through the operation of an unmanned aerial vehicle.” Section 5 of the bill contains exceptions based upon consent, imminent threat to life, search warrant, court order, or for non-evidentiary or non-intelligence purposes. It is difficult to imagine why a law enforcement agency would want to receive drone information that has no evidentiary or intelligence value.


120. FL SB 92, § 1(2)(b).

121. Id. § 4(a)–(c). It also allows drones to be used “to achieve purposes including, but not limited, facilitating the search for a missing person.”

122. Id. § 6.

123. ID SB 1134, § 1 (designating a new section of the Idaho Code as Section 21-213 “Restrictions on Use of Unmanned Aircraft Systems”).

124. Id. § 21-213(2)(a).

125. Id.

126. IL SB 1587, § 10.

127. Id.

128. Id. § 15.
Intersection of Domestic Counterterrorism Operations and Drone Legislation

129. Id. §§ 30, 20, and 25, respectively.

130. Unlike most bills surveyed, the Illinois law specifically acknowledges the applicability of “judicially recognized exception(s) to the exclusionary rule of the Fourth Amendment to the U.S. Constitution or Article I, Section 6 of the Illinois Constitution.” It explicitly states that courts can independently review admissibility for compliance with these constitutions.

131. Id. § 20.

132. MT SB 0196, § 1(1). The Fourth Amendment requires the government to obtain a proper warrant, issued by a neutral and detached magistrate, unless a specifically established and well-delineated exception to the warrant requirement applies. These exceptions include, but are not limited to, exigent circumstances, consent searches, and plain view. For exigent circumstances, see Coolidge v. New Hampshire, 403 U.S. 443, 474–75 (1920) (“it is accepted, at least as a matter of principle, that a search or seizure carried out on a suspect’s premises without a warrant is per se unreasonable, unless the police can show that it falls within one of a carefully defined set of exceptions based on the presence of ‘exigent circumstances’”); Schmerber v. California, 384 U.S. 757 (1966); consent, Schneckloth v. Bustamonte, 412 U.S. 218 (1973); and for plain view as it relates to aerial surveillance, California v. Ciraolo, 476 U.S. 207, 213 (1986); Florida v. Riley, 488 U.S. 445, 448 (1989). The Supreme Court has determined that exigent circumstances exist in the case of imminent danger to life, where a felon or suspect is fleeing and where the destruction of evidence is imminent. Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 298–99 (1967) (“The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others.”); Tennessee v. Garner, 471 U.S. 1 (1985) (law enforcement may use nonlethal force to deter a fleeing felon); Roaden v. Kentucky, 413 U.S. 496, 505 (1973) (“Where there are exigent circumstances in which police action literally must be ‘now or never’ to preserve the evidence of the crime, it is reasonable to permit action without prior judicial evaluation.”).

133. MT SB 0196, § 1(2).

134. Some may argue that state drone laws are preempted by federal law. The topic of federal preemption of state drone laws merits its own article and is beyond the scope of this chapter. Even assuming preemption applies, as a practical matter, a federal officer would have to be summoned into court, request DoJ substitution or representation, and affirmatively assert preemption. The better course of action would be for states to exclude federal officers from their laws from the inception, especially the U.S. military … Apparently, numerous states believe they can legislate federal and military actors’ drone use. However, a plausible argument for preemption would be that the Federal Aviation Act (FAA) of 1958 and its supplements, including the 2012 FAA Modernization and Reform Act, when combined with comprehensive FAA regulations found at 14 C.F.R., illustrate Congress’s intent that the FAA occupy the entire field of aircraft safety. See Thomas J. McLaughlin, Mary P. Gaston & Jared D. Hager, Navigating the Nation’s Waterways and Airways: Maritime Lessons for Federal Preemption Airworthiness Standards, AIR & SPACE LAWYER, Vol. 23, No. 2, Oct. 25, 2010, available at http://www.perkinscoie.com/files/upload/10_27_ABAArticle.pdf. See also City of Burbank v. Lockheed Air Terminal, 411 U.S. 624, 639, 93 S. Ct. 1854, 36 L. Ed. 2d 547 (1973) and Nw. Airlines v. Minnesota, 322 U.S. 292, 303, 64 S. Ct. 950, 88 L. Ed. 1283 (1944) (Jackson, J., concurring).

135. OR HB 2710, § 2(1).

136. Id. §§ 3–7.

137. Id. § 16 for non-applicability to U.S. Armed Forces.

Colonel Dawn M.K. Zoldi

139. Id. § 2(2)(a)–(b).
140. Id. § 5.
141. TN SB 796, § 1(c) (amending TENN. CODE ANN., tit. 39, Ch. 13, pt. 6).
142. Id. § 1(d)(1)–(5).
143. Id. § 1(g)(1)–(2).
144. Id. § 1(f).
147. Id.
148. Id. § 423.003.
149. Id.
150. Id. § 423.005.
151. Id. § 423.006.
152. VA HB 2012, § 1.
153. Id. With respect to the National Guard, VA law states:

The prohibitions in this section shall not apply to the (State) National Guard while utilizing unmanned aircraft systems during training required to maintain readiness for its federal mission, when facilitating training for other United States Department of Defense units, or when such systems are utilized for the Commonwealth for purposes other than law enforcement, including damage assessment, traffic assessment, flood stages, and wildfire assessment . . . .

See also PA SB 875, § 5(1)–(3), which contains identical language. “Title 32” status is usually a “training” status, where the federal government provides training funds to National Guard units.
154. HR 972, § 2.
155. Id.
156. Id. § 4.
157. HR 1262, § 341; HR 2868, § 3(a)(1).
158. HR 1262 & HR 2868, § 341(a)–(b).
159. Id. § 341(b)(3)–(4).
160. Id. § 341(b)(6).
161. H.R. 637—Preserving American Privacy Act of 2013. As do some states, the PAPA also addresses private, or nongovernmental, use of drones. Like CA Senate Bill No. 15, it makes it unlawful to intentionally collect, “in a manner highly offensive to a reasonable person,” images of individuals “engaging in a personal or familial activity under circumstances in which the individual had a reasonable expectation of privacy.” Unlike the California bill, the PAPA fails to describe the remedy for such a violation. Id. § 3119f; CA SB No. 15.
162. Id. § 3119i.
163. Id. § 3119h.
164. Id. § 3119(c)(b)(1)–(5).
165. Id. § 3119(b) and (c). The data collection statement would include the purpose of the operation, whether the drone is capable of collecting covered information, data retention time, a point of contact for citizen feedback, the responsible unit, the rank and title of the person authorizing the operation, and data minimization policies, as well as oversight procedures. HR
Intersection of Domestic Counterterrorism Operations and Drone Legislation

637, § 3119b(c) (1)(A)–(H). This is similar to information required in a DoD PUM. See, e.g., AFI 14-104, Attachment 4.

166. Id. § 3119c(5)(B); § 3119c(1)(B).

167. Id. § 3119c(c)(a).

168. Id. § 3119a(2)(A)–(B).

169. H.R. 1083. Person is defined at 49 U.S.C. § 40102(a)(37) as including “a governmental authority and a trustee, receiver, assignee, and other similar representative.”


172. DoDI 3025.21, Encl. 3, § 5(a)–(b) and Encl. 3, §§ 1, 1c(1)(a)–(g); DoDD 3025.18, ¶ 40 and DepSecDef Memo, Sept. 28, 2006.


174. DoDD 3025.18, ¶ 4.o.


176. See notes 7, 13–14, supra.

177. For a more thorough discussion of state and federal drone proposals, DoD drone policies, and existing constitutional and other principles, in relation to a framework that allows drones to be used to their full potential while protecting personal privacy across all operations, see DAWN M.K. ZOLDI, COL., USAF, DRONES AT HOME: DOMESTIC LEGISLATION—A SURVEY, ANALYSIS AND FRAMEWORK, pending publication and available upon request from the author.

178. See note 20, supra.

179. Id.; see also notes 51 and 56, supra.

180. See notes 19 and 132, supra.

181. Florida, Illinois, and the federal bill use the language, “to forestall the imminent escape of a suspect.” Tennessee allows drones to be used in “searching for a fugitive or escapee” and Texas for “immediate pursuit of a suspect (who may have committed an offense greater than a misdemeanor).” See notes 121, 128, 155, 142, 147, in that order.

182. See note 23, supra, for fleeing felon citations.

183. WI SB 196/AB 203, § 2, 175.55(2).

184. See notes 121, 128, and 164, supra.

185. All the “conspiratorial activities threatening a national security interest also include “conspiratorial activities characteristic of organized crime”: AR HB 1904, § 12-19-104, ¶ (a)(2)(i)(a); HI SB 783, § 1, ¶ 263B–4(1); ME SP 72, § 4504, ¶ 1(A); and MI HB 4455, § 9, ¶ (1)(a).

186. See also note 25, supra.

187. See note 150, supra.

188. See note 144, supra.

189. See respectively notes 131, 53, and 66, supra.

190. See notes 95–96, supra.

191. See note 31, supra, for facial recognition or other biometric matching technology citations.

192. See note 69, supra.
Youngstown Sheet & Tube Co. et al. v. Sawyer, 343 U.S. 579 (1952), Justice Jackson concurring ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum.").

See respectively notes 75 and 81, supra.

See note 138, supra.

See notes 108–09, supra.

See notes 110–12, supra.

CA SB 15, § 14351.

See note 134, supra.

Oregon House Bill 2710, § 16, explicitly exempts the United States Armed Forces, defined as including the Army, Navy, Air Force, Marine Corps, and Coast Guard of the United States; Reserve components of the Army, Navy, Air Force, Marine Corps, and Coast Guard of the United States; and the National Guard of the United States and the Oregon National Guard.


See notes 104–06 supra, for exclusionary rule citations.

United States v. Janis, 428 U.S. 433, 96 S. Ct. 3021, 49 L. Ed. 2d 1046 (1976) (Held that a determination of whether the exclusionary rule should be applied in a civil proceeding involved weighing the deterrent effect of application of the rule against the societal costs of exclusion. Up to that point, the Court had never applied the exclusionary rule to exclude evidence from a civil proceeding, federal or state.)

See notes 40, 43–44, supra.

Appendix A

State Drone Legislation

Alabama (AL), SB 317—“An Act relating to searches and seizures, to prohibit any government agency from using a drone to gather evidence or information . . .” http://openStates.org/al/bills/2013rs/SB317/documents/ALD00014604/

Alaska (AK), HB 159a—“An act relating to the admissibility of evidence through the use of an unmanned aerial vehicle . . .” (Amending AS 09.25; 11.61; 12.45.038; and 18.65), http://www.legis.State.ak.us/PDF/28/Bills/HB0159A.PDF

AK Enrolled HCR 6—http://www.legis.state.ak.us/basis/get_fulltext.asp?session=28&bill=HCR6
Intersection of Domestic Counterterrorism Operations and Drone Legislation


AZ HB 2269—“House Interim Study Committee on Unmanned Aircraft,” http://legiscan.com/AZ/text/HB2269/id/691575


California (CA), Assembly Bill 1327—“Unmanned Aircraft Systems” (Amending Title 14, Section 14350), http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_1301-1350/ab_1327_bill_20130429_amended_asm_v96.pdf,
CA Senate Bill No. 15, http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0001-0050/sb_15_bill_20130627_amended_asm_v94.pdf and
CA Assembly Joint Resolution 6, http://leginfo.library.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AJR6&search_keywords=

Florida (FL), SB 92 (*passed)—“Freedom from Unwarranted Surveillance Act,” http://www.flsenate.gov/Session/Bill/2013/0092


Indiana (IN), SB 20—(Amending IC 35-46-10), http://www.in.gov/legislative/bills/2013/IN/IN0020.1.html

Iowa (IA), SF 276—“An Act relating to the use of an Unmanned Aircraft System by a State or local law enforcement agency,” http://coolice.legis.iowa.gov/Cool-ICE/default.asp?Category=BillInfo&Service=Billbook&menu=false&hbill=SF276
IA H.F. 427—“Use of drones by law enforcement agencies prohibited—exceptions—remedy,” http://search.legis.state.ia.us/NXT/gateway.dll/cl/85th%20ga%20-%20session%201/03___introduced/001___bills/01___house/hf%20042700.html?f=templates$fn=document-frameset.htm&q=drone%20&x=server$3.0#LPHit1

Kansas (KS), HB 2394—“An Act concerning criminal procedure; prohibiting the use of drones by law enforcement agencies,” http://www.kslegislature.org/li/b2013_14/measures/hb2394/

Kentucky (KY), HB 454—“Citizens Freedom from Unwarranted Surveillance Act” (Amending KRS Chapter 500), http://www.lrc.ky.gov/record/13RS/HB454.htm

Maine (ME), SP 72—“An Act to protect the privacy of citizens from domestic unmanned aerial vehicle use” (Leg. Doc 236) (Amending 25 MRSA Pt 12), http://www.mainelegislature.org/legis/bills/display_ps.asp?sn=126&paper=SP0072PID=0;

Maryland (MD), ME HB 1233—“An Act concerning criminal procedure—law enforcement agencies—use of drones,” http://mgaleg.maryland.gov/2013RS/bills/hb/hb1233F.pdf

Massachusetts (MA), SB 1664—“An Act to regulate the use of unmanned aerial vehicles,” http://www.malegislature.gov/Bills/188/Senate/S1664


Minnesota (MN), HF 1620/1706 & SF 1506—“An Act relating to public safety; prohibiting law enforcement agencies from using drones to gather evidence,” https://www.revisor.mn.gov/bills/text.php?number=HF1620&version=0&session=ls88&session_year=2013&session_number=0
Intersection of Domestic Counterterrorism Operations and Drone Legislation

MN H.F. 990—“A bill for an act . . . regulating unmanned aircraft . . .,” http://wdoc.house.leg.state.mn.us/leg/LS88/HF0990.0.pdf

Missouri (MO), HB 46—“Preserving Freedom from Unwarranted Surveillance Act” (Amending Ch. 305 RSMo), http://legiscan.com/MO/text/HB46/id/749046

Montana (MT), SB 196 (*passed)—“An Act limiting the use of unmanned aerial vehicles by law enforcement; and prohibiting the use of unlawfully obtained info as evidence in court,” (Amending 46-1-202) http://data.oip.mt.gov/bills/2013/billhtml/ SB0196.htm


Nevada (NV), S.B 385 and Assembly Bill 507 (appropriations)—http://www.leg.state.nv.us/Session/77th2013/Bills/AB/AB507_EN.pdf and http://www.leg.state.nv.us/Session/77th2013/Reports/history.cfm?billname=SB385

New Hampshire (NH), HB 619—“An act prohibiting images of a person's residence to be taken from the air,” http://legiscan.com/NH/text/HB619/id/719399

New Jersey (NJ), No. 3157—“An Act concerning police surveillance . . .” (Supplementing Title 2A), http://www.njleg.State.nj.us/2012/Bills/A3500/3157_I1.PDF

NJ Assembly Bill 3929—“An Act concerning the use of unmanned aerial vehicles by law enforcement,” http://www.njleg.state.nj.us/2012/Bills/A4000/3929_I1.PDF


NY AO 8091—“Unlawful surveillance by use of a drone,” http://assembly. state.ny.us/leg/?sh=printbill&bn=A08091&term=2013

NY AO 6541—“An Act to amend the civil rights law in relation to the use of unmanned aerial vehicles,” http://assembly.state.ny.us/leg/?sh=printbill&bn=A06541&term=2013


North Dakota (ND), HB 1373 and (2)—“A Bill for an Act to provide limitation on the use of UA for surveillance and to provide for a legislative management study,” http://www.legis.nd.gov/assembly/63-2013/documents/13-0664-02000.pdf?20130520132201

Ohio (OH), H.B. 207—“An act to limit the use of drones by law enforcement agencies and prohibit the defense of sovereign immunity,” http://www.legislature.state.oh.us/bills.cfm?ID=130_HB_207


Oregon (OR), HB 2710 (*passed)—“A Bill for an Act relating to drones and declaring an emergency,” www.leg.State.or.us/13reg/measures/hb2700.dir/hb2710.en.pdf

OR S.B. 524—“Relating to drones and declaring an emergency,” http://www.leg.state.or.us/13reg/measpdf/sb0500.dir/sb0524.intro.pdf

OR S.B. 71—“Relating to drones and declaring an emergency,” http://www.leg.state.or.us/13reg/measpdf/sb0001.dir/sb0071.intro.pdf

OR S.B. 853—“Relating to drones . . . and declaring an emergency,” http://www.leg.state.or.us/13reg/measpdf/sb0800.dir/sb0853.intro.pdf


PA S.B. 875—“Fourth Amendment Protection Act,” http://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2013&sessInd=0&billBody=S&billTyp=B&billNbr=0875&pn=1028

Rhode Island (RI), GA—“An Act relating to criminal procedure: unmanned aerial vehicles” (Title 12 Chapter 5.3), http://webserver.rilin.State.ri.us/BillText/BillText13/HouseText13/H5780.pdf

RI LC00564—“Aerial Privacy Protection Act,” http://webserver.rilin.state.ri.us/billtext13/senatetext13/s0411.pdf

South Carolina (SC), H3415—“Freedom from Unwarranted Surveillance Act” (17-13-180), http://www.scStatehouse.gov/query.php?search=DOC&searchtext=drones&category=LEGISLATION&session=120&conid=7183564&result_pos=0&keyval=1203415&numrows=10

SC G.A. Bill 395—“To prohibit . . . unmanned aerial vehicle containing an antipersonnel device,” http://www.scstatehouse.gov/query.php?search=DOC&searchtext=surveillance&category=LEGISLATION&session=120&conid=7338399&result_pos=0&keyval=1200395&numrows=10

Texas (TX), HB 912—“Texas Privacy Act,” (Title 4, Chapter 423) (*passed), http://www.capitol.state.tx.us/tlodocs/83R/billtext/pdf/HB00912F.pdf


  WV House Concurrent Resolution No. 101—http://www.legis.state.wv.us/Bill_Text_HTML/2013_SESSIONS/RS/Bills/hr101%20intr.htm

Wisconsin (WI), S.B. 196 and Assembly Bill 203—“Relating to restricting the use of drones” (same), https://docs.legis.wisconsin.gov/2013/related/proposals/ab203

Appendix B
Federal Drone Legislation


H.R. 1242—“To prohibit the use of drones to kill citizens of the U.S. within the U.S.” (R. Reid Ribble, R-WI), http://www.gpo.gov/fdsys/pkg/BILLS-113hr1242ih/pdf/BILLS-113hr1242ih.pdf


S. 505—“Bill to prohibit use of drones to kill U.S. citizens in U.S.” (S. Ted Cruz, R-TX), http://www.gpo.gov/fdsys/pkg/BILLS-113s505pcs/pdf/BILLS-113s505pcs.pdf

Epilogue

The Laws of Counterterrorism: What Next?

W. George Jameson

“In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States . . . .”

“Are we done yet?”
— Ice Cube, 2007

The evolution of U.S. policy and application of the laws in dealing with terrorism over the past 20-plus years—from a “criminal” focus to a “war and national security” focus to a “criminal and war and national security focus”—has left many confused about the sufficiency of U.S. laws, policies, and capabilities for addressing counterterrorism challenges. Twelve years after the catalytic events of 9/11, questions continue to arise over whether the United States is doing too little or too much to protect Americans; whether privacy and civil liberties are being violated, otherwise at risk, or neither; and whether organizational responsibilities and legal authorities are inadequate, overbroad, or both. Seemingly, the answer is “yes.”

The public’s continuing national and even international debates about U.S. counterterrorist efforts recently have been evidenced in the frenzied commentaries over the legality, propriety, and efficacy of intelligence-collection efforts epitomized by the National Security Agency’s so-called PRISM and related programs. Both the Bush and the Obama administrations long resisted calls for greater transparency about the legal basis for operations, generally opposing public release of all the legal opinions interpreting the basis for interrogation and detention policies and
the precise rationale for the use of drones to kill terrorists, respectively. Some—mostly, but not only, critics of U.S. policies—allege that there is confusion over the extent of and authorities for ongoing programs. They suggest a need for greater clarity as to both the laws and the principles that govern the U.S. approach to anticipating and dealing with terrorist threats and acts, from collection of information through disposition of those clearly involved in carrying out terrorist activities. In addition, critics and defenders alike assert that it is an open question whether U.S. laws are fully adequate to address the significant challenges the nation faces in countering terrorism and defending national security while protecting civil liberties and privacy interests.

The chapters in this book, like those in its predecessor, *The Law of Counterterrorism*, commendably make significant contributions to an understanding of the laws currently available to address terrorism challenges. The purpose of this epilogue is to highlight issues that warrant attention and to stimulate thinking about the current phase of the post-9/11 era. This period has been described by some as the “new normal”—less frenetic than the period immediately following 9/11, but nevertheless a period fraught with danger to Americans and others in the U.S. and abroad. In this author’s view, future discussions about possible solutions, and any successors to this book, should strive to take advantage of this period of relative calm to contribute to enactment of measures that can ensure clear, transparent policies and laws that address terrorism and homeland security–related problems both comprehensively and, rather than in piecemeal and reactive fashion, proactively.

**The Challenge: Balancing National Security and Civil Liberties Interests**

Following the horrific destruction of the World Trade Center towers on September 11, 2001, Congress and the Executive were pressed to act by the urgent demands of a nation fearing that additional attacks on U.S. soil were imminent. The result, as we know, was enactment of several statutes authorizing swift, adaptable, and direct action to bring the perpetrators and their affiliates to justice. The Authorization for the Use of Military Force (AUMF), PATRIOT Act, Foreign Intelligence Surveillance Act (FISA), and other legislative amendments, along with the creation of the Department of Homeland Security and a new Director of National Intelligence, were measures designed to empower and energize U.S. counterterrorism efforts. They were intended to provide both an organizational framework and requisite legal authorities to meet the challenges and threats ahead. These measures have met with some considerable, although not complete, success. Today, questions still persist and new questions continue to arise over matters relating to the policies and legal authorities and responsibilities to conduct warrantless searches and intelligence gathering, to capture and detain terrorist
suspects or target them for killing, and the appropriate measures for U.S. authorities to bring terrorists to U.S. or foreign tribunals for prosecution and justice.

Some commentators have noted that suggestions to amend the laws sometimes are not much more than reactive, ad hoc proposals to address the most recent specific terrorist acts or alleged government missteps. For example, following one attempted terrorist plot, some urged the U.S. to lower the threshold for inclusion of names of suspected terrorists on the “no-fly list”; ironically, this was not long after calls to limit the inclusion of names. Others have sought legislation to provide for summary loss of U.S. citizenship for terrorists. Also, controversy over whether suspected terrorists could evade justice by refusing to answer questions without having a lawyer present led to calls to modify the requirements for implementing Miranda in order to hold suspects for questioning. Law enforcement practices now implement policies that enable U.S. officials to consider the timing of such “you have the right to remain silent” warnings in questioning terrorist suspects. Concerns over the installation of cameras on city streets have raised privacy interests, but those concerns became somewhat muted following the attacks at the Boston Marathon after street cameras, admittedly private and not government-owned, led to the speedy identification of suspects.

The government has touted its successes in preventing terrorist acts by citing to its use of electronic surveillance capabilities under the Foreign Intelligence Surveillance Act (FISA) enacted in 1978. That act was amended after 9/11 to enable intelligence and law enforcement authorities to collaborate more effectively in gathering and sharing intelligence. Officials from both the executive and legislative branches note the value of these authorities, including the much-publicized sections 215 and 702, which provide authority for broad collection of data without need to identify specific targets. They further note that the measures are a statutory response to the pressures to do more to identify and locate terrorists. Others cite civil liberty concerns that such efforts have gone too far. At least one noted authority has argued that the measures are unconstitutional, even if they are legally authorized by statute.

Debates over the legality and propriety of national security operations should not be surprising. As this author has heard a former CIA director say to an ABA audience, “When Americans are afraid, they want CIA to do more; and when not afraid, they think we are doing too much.” The government deals with such situations as they occur, typically justifying what it has or has not done under existing legal authorities while seeking ways to modify and improve its practices to deal with the next case that raises those same scenarios. Sometimes, when there is time for reflection, officials seek to anticipate needs and provide statutory bases that are not simply reactive. Often, the focus of such efforts is driven by ever-increasing technological advances that threaten U.S. security. Typically
standing in the way of change are either secrecy, concerns with civil liberties or unintended consequences, or bureaucratic or other priorities.

As other authors in this book indicate, calls for creation of a new “terrorism court” suggest to some an alternative to the confusion that can result from having to choose whether to bring suspects before Article III courts or military commissions. Congress and the President agreed on a special court to deal with electronic and, later, physical surveillance, and military commissions have operated since long before the post-9/11 establishment of commissions for detainees. Accordingly, a special court to prosecute terrorists provides a new but not unprecedented option for handling such cases properly and securely. Yet, 35 years after its establishment pursuant to the FISA, the so-called FISA court, or FISC, has become embroiled in controversy for approving— in secret, but absent any actual proof of wrongdoing or illegal action—government collection and amalgamation of vast amounts of data that pertain to the activities of Americans. Some assert these actions have, even if legal, crossed the boundaries of what this nation should do—in the hunt for foreign terrorists who would attack U.S. interests and kill citizens and others. Others note a need for greater transparency into the processes and legal rationale, and further claim that the non-adversarial nature of FISA proceedings violates due process and is in need of change.

Concerns about ensuring protection of national security, equal justice under the law, and other important principles were heightened when senior officials urged public trial in federal court and not before a military commission. One official publicly remarked without elaboration that the U.S. authorities might not release certain terrorists even if they are acquitted in an Article III court. To those familiar with the laws of war, the notion that prisoners can be held until war’s end is not new. To those more comfortable with the criminal justice system’s handling of violations of U.S. criminal law, the concept is disconcerting to say the least, particularly when there is no clear sense of when or if hostilities will end.

Similarly, many have expressed concern that the U.S. government could and would target an American citizen for a drone strike without a judicial or some other public due process proceeding. The lack of full transparency over the legal rationale and factual basis for doing so fuels those who believe these, if not all, drone activities are ill-considered, counterproductive, and illegal. This view persists despite the Administration’s public presentations—from senior officials in the State, Justice, and Defense departments as well as the National Security Council staff—of legal rationales that articulate the U.S. position. In large measure, the continued secrecy surrounding these activities, including the continued classification of legal opinions and court rulings, hinders full acceptance of the government’s rationale.
Secrecy can present conflicting concerns. Although some profess to disagree, it is clear at least to this author that leaks of classified information can be damaging. Debates persist, and have probably always existed, over whether disclosures of classified operations are treason, other perfidy, or honorable whistle-blowing. The government’s episodic successes and failures to take steps to identify and punish those who have, for whatever motive, violated their sworn oaths of secrecy further erode confidence in the reliability of the government, its promises to agents and allies, and, when members of the press are investigated or questioned, the inviolability of a free press.

Reliance on statutes designed to punish foreign espionage as the primary means of prosecuting those who leak secrets to the media strikes some as only fitting, as President Truman noted that such leaks can be as damaging as espionage. In 2001, DCI Tenet urged the need for comprehensive leaks laws to facilitate identification and punishment of leakers. This could remove the espionage stigma from those who might be disloyal, but not spies for hostile foreign governments so much as enablers of a commercial press or other real or perceived legitimate cause. As a nation, we have not yet determined how to balance the need for a free press with the need for government secrecy to protect sensitive counterterrorism operations that have been disrupted and even discontinued by the revelation of their existence.

Secrecy that protects and enables an effective U.S. response to terrorism also can stymie redress efforts of innocent persons harmed by acts of terrorists, as well as others who allege they have been harmed by U.S. counterterrorist activities. “State secret” privilege claims fuel the outrage of those who question U.S. actions and values when courts decline to hear cases brought by claimants alleging they have been wrongfully accused of being terrorists and subjected to physical and mental abuse and, as a result, lawfully denied remedial action. Remedies normally available to U.S. citizens are not always available under the law to adjudicate civil liberties claims when national security interests are present. Rulings that deny a claimant’s action to proceed because of government secrecy deny access to information that could, allegedly, show the harm caused. This can lead to further frustration with, if not distrust of, a government that they see as so uninterested in righting real or perceived wrongs that it would not even allow inquiry into the matter. Nevertheless, such is the state of the law, and so it has been from early in the history of our nation. And for those more concerned with equity than with law, the fact that redress might be available from private bills enacted by Congress offers little comfort.
The Congress recognized when it enacted the National Security Act in 1947 as a reaction to the surprise attack at Pearl Harbor that it is important to ensure that the U.S. approach to dealing with national security interests is appropriately comprehensive. U.S. laws should provide a broad framework to anticipate, detect, prevent, and counter terrorist threats and attacks against the United States and other U.S. national security interests. Transparent policies and legal approach would enable appropriately integrated U.S. actions to identify and bring terrorists, their sponsors, and their surrogates to justice in the U.S. or abroad and, perhaps, deter terrorist acts and their underlying causes. Understandably, perhaps, the U.S. solutions to terrorism concerns since 2001 have been largely reactive, as was the reaction to Pearl Harbor. It is time for an assessment of the adequacy of U.S. laws and policies to deal with terrorism both comprehensively and, to the extent possible, in an anticipatory fashion. As others have noted, this is best done by Congress and the Executive rather than left to the courts to address on an ad hoc basis.

In reviewing the adequacy of the laws relating to counterterrorism, several elements must be considered, including organizational structures, authorities, and relationships; tools for collection and analysis of information; and clear guiding principles. In addressing these matters, it might be useful to think in terms familiar to most junior high school students who have been told by their English teachers to be sure their school essays address “who, when, where, what, how, and why.”

Who Should Do What: Form Versus Function

Much of the early debate regarding counterterrorism challenges has been directed at the “who”—which elements of the U.S. government should conduct particular operations. This is a typically bureaucratic approach, but one with operational implications if not imperatives. The Title 10 versus Title 50 discussions focus on whether the Department of Defense (DoD) and the military or, instead, the Central Intelligence Agency should have responsibility for paramilitary operations— for example, to conduct drone operations that target terrorists. Following proposals to consider transfer of paramilitary capabilities from CIA to DoD, the Bush Administration rejected that option after extensive interagency review. Moreover, as the successful UBL operation showed, a merger of the two can be highly effective. Yet questions persist. The answers, however, should depend less on bureaucratic organizational charts and more on which element has the capabilities to operate effectively in a particular situation to carry out the U.S. policies, goals, and objectives. In the sliding scale from covert (that is, non-attributable) action to
open war, there is much gray area and room for debate over “who” should conduct an operation and why.

Similarly, renditions have long been a tool in the U.S. arsenal of options to bring criminals to justice. Whether they or other national security–related operations should be conducted solely by law enforcement or also by intelligence and military organizations precluded from having domestic law enforcement functions raises the question of the roles of law enforcement agencies in national security affairs. Amendments to FISA since 9/11 have been designed to improve collection capabilities against known or suspected terrorists, to detect unknown actors, and to enhance collaboration among intelligence and law enforcement agencies. This adjustment of authorities followed decades of enforcing varying degrees of separation between law enforcement and intelligence activities. This dynamic was driven by post–World War II fears that demanded that the new central intelligence organization, the CIA, not be a Gestapo-like entity that merged foreign and domestic responsibilities and, more dangerously, exercised authoritarian powers. Even within any of the three intelligence and national security communities (that is, the national intelligence, law enforcement, and military communities), jurisdictional lines are sometimes unclear. For example, the demarcation lines for FBI and Department of Homeland Security responsibilities in the U.S. continue to lack precision as each element continues to refine its role for investigating and handling domestic homeland security–related threats and coordination with state and local authorities.

Some private efforts, like those of the Project on National Security Reform, have suggested consideration of an approach that ensures “unity of effort” as well as, in appropriate cases, “unity of command.” This assumes as a basic premise that the U.S. as a whole has the capacity and authority to combat terrorism, but that dispersal of command and control reduces U.S. effectiveness and efficiency. A “unity” approach would revamp how operations are managed and redefine the role of the NSC as well as centralize oversight responsibilities of several congressional committees. Under this formulation, it shouldn’t really matter who takes action so long as the full authorities of the U.S. are appropriately available and there is, as in the military model, someone in charge. Critics sometimes note that overseas the ambassador does not control the combatant commander nor, for that matter, the CIA’s chief of station. On the other hand, it is not clear how a diplomat would effectively command troops in combat or coordinate the activities of spies.

This largely organizational issue involves legal, policy, and bureaucratic constraints that hamper effectiveness but also reflect a dynamic dictated by our national “DNA” that recognizes and values a separation of powers among the three distinct branches – legislative, executive, and judicial. A similar constitutional
dynamic exists in how our nation distinguishes federal and state powers and responsibilities; not all power resides in one place. Tensions, therefore, are inherent in our system—a system designed in part to ensure that government conduct is constrained where necessary, even if this results in bureaucratic inertia, or worse.

Distinguishing military, intelligence, and law enforcement roles may appear to be unduly bureaucratic and inefficient, but also can provide necessary safeguards to protect the people from the risk of an overly powerful central organizational entity. The CIA is not authorized to perform law enforcement functions—a guard against another “Gestapo” that leaves to law enforcement experts the job of bringing criminals to trial; the Posse Comitatus Act precludes the military from exercising law enforcement authorities in light of experiences in post–Civil War politics; more recently, use of special collection authorities under FISA demands that do not envision adversarial, public proceedings are not permitted where the only interest is law enforcement. Also, some would recall the fears raised when the Department of Defense was established in 1947. Initially named the National Military Establishment, or NME, the name was changed upon realization that its pronunciation—“enemy” for NME—inappropriately suggested a powerful and sinister force. Today the FBI has both law enforcement and intelligence missions, and the military plays a lead role in countering terrorism. Any debate over “who” should do what to counter terrorism would be well-served by an examination of all these roles to guard against, or to ensure effective management of, any aggregation of power that could, left unchecked, run counter to the values and system upon which our nation is based.

Oversight

Another aspect of who should do what involves the important question of oversight responsibilities. Government agencies face multiple layers of oversight, both internal and external: agency counsel, inspectors general, the National Security Council, the President’s Intelligence Advisory Board, House and Senate committees, the courts and, unofficially, the press. The President’s Privacy and Civil Liberties Board has been recently constituted to help balance national security and civil liberties interests.

With respect to Congress, the intelligence committees have oversight responsibilities regarding covert action; the armed services committees for military operations; judiciary committees for law enforcement; foreign affairs committees for State; and for Homeland Security, it has been said that more than 100 committees and subcommittees of Congress have interests in overseeing DHS. Oversight typically hinges on which U.S. element conducts an activity. If operations merge, or if authorities for the conduct of operations are dispersed, oversight responsibilities become murky, with a potential for overlap as well as gaps. More
important, perhaps, than which element is to be overseen will be the nature of the activity if the consequences—operational, diplomatic, military, or economic—are likely to be the same. The question of who—that is, which element of Congress, if any—has cognizance over the totality of U.S. counterterrorism efforts should be given careful consideration in any effort to establish a comprehensive counterterrorism approach.

When Should the U.S. Act?

Regardless of which agencies of government have particular authorities for counterterrorism activities, an important question asks “when” the U.S. should act. From the perspective of the United States (as opposed to that of our foreign allies whose citizens the U.S. might target), intelligence and other agencies should always collect information relating to the capabilities and intentions of foreign countries, their agents, and persons when the threat of terrorism is at stake. Nevertheless, some have pointed out a need to define “terrorism” in light of the distinctions between international terrorism and local terrorist acts that do not cross international borders but are strictly local matters. It should be clear when acts of terrorism should justify U.S. attention and response.

With respect to U.S. citizens or others within the United States, what is the “trigger” that should permit the collection of information to determine if a person is a terrorist? How long must the U.S. government, or, for that matter, the New York Police Department or other local authorities, wait before attempting to gather information through infiltration of social or religious groups? What are the limits on acting if a terrorist threat exists or could develop when the so-called triggering activity also can be seen as a legitimate exercise of First Amendment rights? How should the fears of rights violations or other harm affect law enforcement practices that could include data mining when the issue is not a matter of connecting the dots but requires finding the dots to begin with? What use should be made of drones over the United States, as the FBI recently acknowledged, or profiling to prevent action, as opposed to simply finding, in a more traditional law enforcement approach, the perpetrators of acts already committed? More direct targeting of specific individuals raises other concerns that warrant discussion and clarity, such as when the U.S. may target for lethal action an American or, for that matter, any other person who is involved in activities that pose a threat to U.S. persons or national security interests.

The laws of war and the criminal code each offer some answers for those who ask when the U.S. may act, depending on the context, and further exploration of these legal vehicles and the appropriateness of their use will be essential to help guide counterterrorism leadership in determining when to act in our nation’s interests.
The distinctions between law enforcement and intelligence functions have carried with them the general rule, albeit not absolute, that typically delineated the roles of U.S. government agencies as domestic (the FBI’s domain) versus foreign (a CIA focus). Whether and how an intelligence agency operated depended upon whether the persons or threats were domestic or foreign-based. Moreover, development of the law established legal parameters depending upon whether the target was an agent—usually but not always abroad—of a foreign power. This often reflected a determination whether the purpose of the collection was to advise policymakers who set policy or to take counterintelligence measures against foreign States or their agents, or whether the purpose was to take action against specific persons, such as to prosecute an individual in open U.S. court proceedings for violation of the criminal code. The former permitted use of more extraordinary authorities with fewer requirements for judicial review and carried less of a risk that collection of information would violate rights of U.S. persons. The latter, however, involved specific targets, often U.S. persons whose constitutional safeguards demanded observation of additional formalities and presentation of evidence in an adversarial open court proceeding. Espionage cases, to be sure, always presented elements of both categories.

In general, therefore, collection of intelligence has been described in terms of collection inside and collection outside the United States, at least following the establishment of Attorney General procedures governing each intelligence element pursuant to the series of executive orders governing their conduct. The resulting dotted or virtual line at the border, however, has less meaning today in light of technological advances whereby communications move back and forth across borders. This can make the inside-outside distinctions almost meaningless, especially when the war on terror, or perhaps more properly the war waged by terrorists, has made the battlefield global. If this is the case, then the historic questions of who acts and where become more difficult to address.

- The military fights wars abroad but has a domestic (NORTHCOM) presence to protect the homeland.
- The FBI, as both a law enforcement and intelligence agency, has a domestic focus, but its counterterrorism mission demands overseas insights and, as in the past, the capability to exercise its responsibilities in conjunction with foreign partners abroad.
- The NSA’s collection activities target communications that may or may not implicate the rights of U.S. persons, and questions of whether the “ether” where its collection might occur increasingly pose challenges in
determining the adequacy and currency of laws designed to function based on technologies of the past.

• The CIA’s role, as a foreign intelligence agency with covert action responsibilities, enables it to operate uniquely abroad without the role of the U.S. being acknowledged or apparent, and to operate in collaboration with its foreign partners in ways that other U.S. elements cannot. At the same time, although constrained in collection activities by directive, the CIA collection activities in the U.S. are not expressly precluded by statute. Nor is it suggested they should be, as the opposite might be true.

• As with the discussion of organizational roles and how functions within the government are assigned to handle a specific mission or challenge, the concept of unity of effort and unity of command warrant consideration of whether legal impediments exist that demand a “handoff” of activities once a threat moves across the U.S. border, regardless of direction.

**What Can the U.S. Do and How?**

These two categories—what and how—will be intertwined for purposes of this discussion. They strike at the heart of the debates about the legality and propriety of U.S. counterterrorism activities, such as:

• Analysis of social media to identify illicit or threatening activities.
• Acquisition of email and telephone records.
• Use of National Security Letters to obtain otherwise private financial records.
• Aggregating data to detect patterns to identify financial or weapons transactions and terrorists.
• Diplomatic or economic measures to counter terrorists or enlist support.
• Overt use of military elements to engage a ruthless and unrelenting adversary.
• Employment of covert capabilities to counter threats or influence potential allies.
• Strikes targeting specific terrorists or groups of persons presumed to be threats.

These activities, and more, must proceed on a sound legal basis. The AUMF will be of limited utility as the threat of Al-Qaeda and its affiliates diminishes and their threats are replaced by others. Developments in the case law, as seen in the Supreme Court’s Jones decision rejecting the government’s analysis about authorities to track vehicles, similarly suggest ambiguity regarding the extent of current authorities. Moreover, as noted, debates about FISA have included questions about
whether activities are appropriate—and whether the gain is worth the pain—even if they are legal.

Unmentioned in this epilogue thus far, but by no means insignificant, the challenges of cyber threats also bring with them the need to ensure clarity both for the government and the state, local, and private-sector partners on whom the U.S. must rely so heavily. To date, there has been limited movement toward a statutory cyber framework that would be acceptable to Congress, the Executive, and the private sectors alike. Finding solutions to cyber threats will require weighing civil liberties, privacy, and, increasingly, financial and economic interests.

Unquestionably, the questions of legality have particular meaning for citizens and others who are the targets of U.S. counterterrorism operations. Another constituency eager to ensure clarity of authorities, however, is that comprising the government officials, contractors, and others who support the U.S. government’s efforts. Those persons who act in good-faith service to their country expect they will be protected by laws, directives, and guidance that permit them to understand what they may do and how, and with the assurance that what they understood was lawful conduct would not subject them to years of second-guessing or lead them to bankruptcy in defending themselves during legal proceedings in the U.S. or abroad. It is for this reason that a necessary element of this discussion should address the need for a clear framework for appropriate, not carte blanche, grants of immunity.

**Why Would the U.S. Act?**

In its simplest terms, of course, the U.S. acts to protect itself and its citizens and interests. Whether a particular action is necessary will depend on the circumstances, but it would be useful to articulate basic principles and core authorities that are a little more specific than the language in the U.S. Constitution. Under executive order procedures for intelligence collection, agencies are required to utilize the least intrusive means necessary to gather information on U.S. persons. Debates over the effectiveness of PRISM and related programs ask whether collection of less data, or shorter retention periods, would better serve civil liberties interests. The AUMF authorizes military force as a response to the World Trade Center attacks in 2001, but as the Al-Qaeda threat either diminishes or morphs into something else, there will be a need to clarify the basis for future military actions. In the absence of clear statutory authority, it is likely that presidential authority will surface again as the default basis for action, with all the attendant debates about legality that this would entail.

Legal scholars might, repeat might, appreciate the basis for secret U.S. actions, but the global impact of terrorism and counterterrorist activities brings with it not just a clash of state and non-state actors but of different cultures, laws, and legal
principles. For all that we might think the world is “flat,” the respective laws and underlying principles that govern the U.S. and other nations differ, so it will be important to articulate basic principles for a foreign, not merely a U.S., audience.

- U.S. notions of privacy differ from those of many if not most European nations;
- State sovereignty as seen by China and Russia guide their actions with respect to, for example, Syria in ways that run counter to the U.S. view;
- The U.S. authority under the *Ker-Frisbie* doctrine to bring felons before a tribunal without a warrant so long as the government’s conduct does not shock the conscience is considered unacceptable to some other nations;
- In contrast, trials in absentia, not favored in the U.S., seemed to raise no eyebrows in Italy’s prosecution of U.S. officials on charges of abducting a terrorist from Italian soil; and
- Hearsay admissibility under the rules of the Yugoslav war crimes tribunal and International Criminal Court seem to go beyond what U.S. law would consider constitutionally acceptable.

Although treaties are the law of the land, commentators have noted the uproar over any actions by U.S. judges to cite to international law as appropriate legal authority for a judicial ruling. Nevertheless, as terrorism and cyber increasingly reflect their global reach, measures that cross national boundaries will have to be utilized or instituted, and international cooperation may be essential. Perhaps this will involve the use of the ICC as a means of detaining terrorists. Perhaps there is a need for new bilateral or international treaties. Perhaps legal principles will be established that treat international terrorists like, for example, pirates or criminal racketeers and that lead to a RICO-like structure to prevent, detect, and sanction terrorists.

Regardless, it seems likely there will be a need for the U.S policymakers to establish a legal rationale for what we do and why that will help assuage our foreign allies. Although this might not necessarily result in uniform acceptance, at the least our objectives and principles should be presented in terms so clear and unequivocal that there will be no doubt or confusion as to the reasons for our actions, their underlying legal basis, and, hopefully, the propriety of their adoption. It has been said that fanaticism is doubling one’s efforts when one has forgotten one’s goals. There can be no doubt about U.S. resolve in countering terrorism. It will be important to continue to identify and affirm those goals and to articulate them and their legal basis clearly, unequivocally, and comprehensively.
Conclusion

Experts from the law enforcement, military, intelligence, and domestic communities appear to understand and take comfort from the laws that enable them to address terrorism-related problems within their respective areas of responsibility and expertise. What is less obvious is whether either an overlap or a gap in laws and authorities exists to hamper more effective and collaborative U.S. efforts across these communities. One approach to ensuring a comprehensive approach to addressing counterterrorism interests is through a series of events or public discourses to address the adequacy of U.S. laws. These events could convene experts from across several relevant issue areas to discuss the intersection of or any gaps in their respective abilities to address terrorism-related matters and to ensure a comprehensive U.S. approach. Participation would include nonpartisan, expert professionals who currently or previously held government positions as well as others with no prior government experience. A similar effort has been undertaken by the American Bar Association’s establishment of a cyber task force; that is a useful model to be considered.

Events could consist of panels of legal and policy experts from the law enforcement, military, intelligence, diplomatic, and civil government communities, as well as private-sector participants from the academic, civil liberties, media, and commercial communities. They would address, for example:

- Information collection and sharing in light of privacy, civil liberties, or other domestic considerations; authority of the government over the private sector.
- Considerations in targeting terrorists for apprehension, interrogation, and detention in light of the availability of Article III courts and military commissions; implications of criminal law and laws of war.
- Liability of federal officials and their agents in the United States and abroad.
- International collaboration and whether new arrangements are needed.
- Foreign aid and assistance policies and laws and any impact on root causes of terrorism as well as counterinsurgency implications.
- Immigration and other border laws and responsibilities and their impact on counterterrorism capabilities.
- Adequacy of U.S. laws and policies to provide remedies either to persons aggrieved by alleged U.S. improper conduct or to persons harmed by terrorist acts.
Actions taken as a result of these efforts would be part of the incremental process that has included measures such as the PATRIOT Act’s provisions to facilitate collaboration between law enforcement and intelligence, amendments of the FISA, reorganization of the FBI, and, more recently, the review of communications privacy laws and cyber authorities in light of rapidly changing technologies.

The authors in Chapter 1 superbly indicate that there is a need to address political, social, and economic factors that contribute to the causes of terrorism and make countering terrorism so difficult. As subsequent chapters suggest, it also is important not to restrict the focus to military or counterinsurgency interests. For this reason, efforts to counter terrorism will also, as the drafters of the PATRIOT Act recognized, rely upon appropriate disposition of changes to immigration laws, air- and sea-port security, and increasing use of biometric capabilities that can detect hostiles seeking to enter this country but also can identify clandestine U.S. operatives seeking to penetrate hostile elements abroad.

A coherent, cohesive strategy will be essential in the years ahead, and a comprehensive legal regime will be essential. That said, it will be important to keep in mind that there will be no quick or simple solution. This author has no illusions about the enormity of the task, and we should expect that the question raised in the first chapter—“Why is countering terrorism so difficult?”—will continue to present itself well into the future. Nevertheless, this book and the fine work of its editor, Lynne Zusman, in highlighting issues and challenges of terrorism add valuable insights to the discussion and, perhaps, will help make the task a little less difficult.
Additional Information

• First Amendment
• Fourth Amendment
• Post 9/11 Legislation
• Homeland Security Act
• National Security Act, as amended
• Executive Guidance & Direction
• Executive Order 12333 – Basic Charter
• Executive Order, Statute and the 4th Amendment
• Information Sharing and Protection
• Leaks and Related Issues
First Amendment

• “Congress shall make no law . . . Abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble . . .”

• Alien and Sedition laws and surrounding debates show issues are not new

• Free Speech protections of the First Amendment not absolute
  ➢ “No one would question but that a government might prevent actual observation to its recruiting efforts or the publication of the sailing dates of transports or the number and location of troops.” Near vs. Minnesota (1931)
  ➢ Marchetti and Snepp cases upheld prior restraints
  ➢ Progressive (1979) – restrained publication of information released in error, withdrawn from public
Fourth Amendment

• “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probably cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
Post-9/11 Legislation to Enhance Information Capabilities

• USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001), Protect America Act, others --
  ➢ Amended FISA allow “roving taps” when phones switched
  ➢ FISA standard changed – collect when foreign intelligence is "a significant purpose" vs "the purpose"
  ➢ Amended criminal, banking, financial privacy, and immigration laws
  ➢ Authorized sharing law grand jury and wiretap information

• FISA and Sections 215 and 702: Debates over the law as it is versus “should” be
Homeland Security Act of 2002

• Intelligence and law enforcement roles expanded to protect homeland – established intelligence capability
• Gather and integrate all information to identify threats and issue warnings – Note other IC centers
• Develop comprehensive national plans to protect critical infrastructure
• Broad access to information except as otherwise directed by President
• Secretary consults with DNI to ensure dissemination of terrorism information
National Security Act of 1947, as amended by IRTPA (Intelligence Reform and Terrorism Prevention Act of 2004)

• DNI and Office of the DNI
  ➢ Management of the Intelligence Community
  ➢ National Centers
• Independent Agency -- CIA
• Elements within departments
  ➢ DIA, NGA, NRO, NSA
  ➢ Elements in DoD, FBI, State (DEA, later)
  ➢ Elements in military services

Copyright (c) W. George Jameson February 2015
Executive Guidance and Direction

- Executive Orders – Force of Law
  - Specific to IC, law enforcement, others
  - Generally applicable across Government
- Presidential and NSC directives
  - National Intelligence Authority Directive, NSCID, NSPD, PD, PDD
    - Presidential Policy Directive (PPD) 1 sets forth
    President’s policy system today
- Military Directives
- IC/DNI Directives
  - Intelligence Community Directives (ICDs)
- Agency and Departmental Regulations
Executive Order 12333 -- Basic Intelligence Community “Charter”

- Origins date to 1976 and successor orders
- Establishes IC organization and management
  - DNI authorities clarified in 2008 amendments
  - Responsibilities of department heads and IC elements
- Establishes operational authorities, restrictions
  - Collection, retention, dissemination of information on US persons
- Prohibits or limits certain other activities
  - Assassination, human experimentation, covert action in US
- Restrictions apply to all US elements, even those outside the IC, conducting intelligence activities
Executive Authority, Statutes, and the Fourth Amendment

- Inherent authority enables warrantless spying
  - Inherent presidential authority recognized to authorize warrantless searches for national security purposes -- Roosevelt authorization for FBI (1939)
  - *Butenko* and other cases recognize foreign affairs exception to warrant requirement

- FISA legislation imposed statutory requirements for certain electronic surveillance and searches, but
  - Terrorist Surveillance Program (TSP) challenged view that FISA warrants were required
  - *Jones* case addressed privacy expectations
  - Wiki and Snowden leaks invited questions about approved collection of certain phone and email records (PCLOB review)
Intelligence Sharing and Protection

- Executive and IRTPA provisions to improve information sharing followed 9/11 and Iraq WMD
  - President increased sharing of terrorism information
  - DNI to ensure timely dissemination to President, department and agency heads, Congress, Joints Chiefs and senior military commanders
  - DNI has access to all national intelligence unless President decides otherwise (law enforcement exception as DNI and Attorney General decide)

- National Security Act and Executive Orders provided requirements and standards over several decades
  - Collect, classify, and share -- need-to-know/responsibility to provide
  - Aggregations of information
  - Protect sources, methods
Leaks and Related Issues

• Leaks as damaging as treason (Truman)
• Stopping leaks
  ➢ Document protection, tracking
  ➢ Periodic security investigations to identify threats
  ➢ Challenges posed by “responsibility to provide”
• Identifying and prosecuting leakers – adequacy of the laws
  ➢ 18 US Code 793 – communication to one not entitled to it
  ➢ 18 US Code 794 – disclosure to agent of a foreign power
  ➢ *Morison* case civilian prosecuted for providing picture (“Janes”)
• Reliance on espionage laws -- proof and optics challenges
• Contending with the Press and Civil Liberties Concerns
  ➢ Damage from publication of leaks vs. damage from spies
  ➢ Pentagon Papers case (1971) – only limited deference
  ➢ Wikileaks and Snowden challenges