Drones, Technology & Markets: Caught in the Crosshairs of Federal Regulators & Cyber Spies

ABA Showcase Program
Drones Incoming!
Chicago, IL

David Z. Bodenheimer
Crowell & Moring LLP
August 1, 2015
Drones in the Crosshairs

Drone Markets, Regulators & Spies

1. Drones, Technology & Trends
2. Federal Regulators & Risks
3. Drone Spies & Cyber Espionage
UAS – 98 Years

“U.S. military tested the unmanned Kettering Aerial Torpedo with pre-set flight controls in 1917.”

“The global market for nonmilitary drones has already ballooned into a $2.5 billion industry, one that’s growing 15% to 20% annually.”
[“Get Ready for Drone Nation,” Fortune (Oct. 27, 2014)]
Global $91B Market

“Global spending on drones is expected to total almost $91 billion over the next decade. This is the most dynamic segment of the aerospace sector, according to the Teal Group.”

(Hollinger, “Parcel drones face long wait for delivery date,” Financial Times (June 12, 2015))

EU’s UAS Markets

- 2,495 EU drone operators – largest worldwide operations (Forbes, Mar. 23, 2015)
- $17 Billion a year by 2020 – EU civil unmanned systems (The Week, May 17, 2015)
- 10% of EU Aviation Market (Crunch Network, Apr. 25,
Commercial Markets

Table I. Nonmilitary UAS Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Border surveillance</td>
<td>Pipe/power line surveillance</td>
</tr>
<tr>
<td>Suspect tracking</td>
<td>Agricultural applications</td>
</tr>
<tr>
<td>Traffic monitoring</td>
<td>Communications/broadcast</td>
</tr>
<tr>
<td>Disaster response/relief</td>
<td>Movie production</td>
</tr>
<tr>
<td>Damage assessment</td>
<td>Aerial news coverage</td>
</tr>
<tr>
<td>Atmospheric/weather research</td>
<td>Mail/freight transport</td>
</tr>
<tr>
<td>Critical infrastructure monitoring</td>
<td>Flood mapping</td>
</tr>
<tr>
<td>Damage surveying</td>
<td>Real estate mapping</td>
</tr>
<tr>
<td>Aerial photography</td>
<td>Mining</td>
</tr>
<tr>
<td>Wildlife monitoring</td>
<td>Sporting events coverage</td>
</tr>
</tbody>
</table>


Commercial Work

- **Amazon** – home delivery systems
- **Facebook** – internet access
- **Bechtel** – construction monitoring
- **BP** – gravel-extraction monitoring
- **Yamaha** – crop dusting & seeding
- **Rio Tinto** – site safety inspections
- **Warner Bros** – movies & TV
- **Walmart** – UAV cameras
- **Allstate** – insurance inspections
Are Federal Acquisition Regulators Coming After Your Drones?

Your Rights Gone?
Federal Contracting & Commerciality

Rule # 1: Buy Commercial First!  #1

- Federal Acquisition Streamlining Act (Pub. L. 103-355) (Congressional intent for leveraging commercial markets)
- 10 U.S.C. § 2377(b):

  “The head of an agency shall ensure that procurement officials in that agency, to the maximum extent practicable – (1) acquire commercial items or nondevelopmental items other than commercial items to meet the needs of the agency . . . .”
Rule # 2: Cut the Red Tape!

“Such list [of contract clauses for commercial items] shall, to the maximum extent practicable, include only those contract clauses – (A) that are required to implement provisions of law or executive orders applicable to acquisitions for commercial items . . . ; or (B) that are determined to be consistent with standard commercial practice.”

Pub. L. No. 103-355, § 8002 (emphasis added); see also Federal Acquisition Regulation 12.301(a) (same)
Priority of Commercial Rules

Rule # 3: Commercial Trumps All!

“When a policy in another part of the [Federal Acquisition Regulation] is inconsistent with a policy in this part [for commercial items], this part 12 shall take precedence for the acquisition of commercial items.”

Federal Acquisition Regulation 12.102(c)
(emphasis added)
Rule # 4: Protect your IP!

“Except as provided by agency-specific statutes, the Government shall acquire only the technical data and the rights in that data customarily provided to the public with a commercial item or process.”

Federal Acquisition Regulation 12.211 (emphasis added)
Drone Technologies

Drone Technology Multiplier

- **Data Analystics.** “Where will the next trillion files be created? Broadly: the Internet of things. But **UAVs** in particular are going to be a **massive source** of that information.” [“Get Ready for Drone Nation,” *Fortune* (Oct. 27, 2014)]

- **Technology Fusion.** “The advent of cheap 3-D printing of drone parts, open-source software and **cloud computing** has let start-ups like Skycatch jump in.” [“Drones are Becoming Energy’s New Roustabouts,” *NYT* (Apr. 21, 2014)]

- **3-D Printed Drones.** “A team of researchers from the University of Virginia in August debuted the Razor – a small, 1.8-pound UAS with an airframe constructed of nine **3D-printed parts** that join together to **form a flying wing.**” [“Military Technologies that Will Change the Game,” *National Defense* (Nov. 2014)]

- **Jam-Proof Communications.** Laser communications (free space opticals) may allow “jam-proof, reliable communications” where “the commercial sector is leading the world and the nation in this technology.” *Id.*
How Do You Know When Your Drone Technology is a Cyber Target?
Cyber War on Drones

- **Who’s Stealing your Technology?**
  - China, Russia and even our allies

- **What are the Primary Targets?**

  Of the aerospace and aeronautics technologies, “[t]he greatest interest may be in UAVs because of their recent successful use for both intelligence gathering and kinetic operations in Afghanistan, Iraq, and elsewhere.”

Office of the National Counterintelligence Executive (Oct. 2011)
Technology Targets

“77% increase in the number of reports targeting aeronautics systems.”

“Within the category [of aeronautics technologies], collection reports focused on unmanned aerial vehicles (UAVs), including micro-air vehicles.”

[DSS, Targeting U.S. Technologies (2013)]
Cyber Risks – DoD Rule

Key Requirements

- **Scope**
  - “controlled technical information”
  - *E.g.*, R&D data, specs, standards, drawings

- **Minimum Security Controls**
  - 51 mandatory controls (NIST 800-53)

- **Incident Reporting**
  - Within 72 hours of discovery
  - Damage assessments & data retention

- **Subcontractor Flowdown**
  - Commercial contractors also

DFARS Cyber Rule

DEPARTMENT OF DEFENSE
Defense Acquisition Regulations System
48 CFR Parts 204, 212, and 252
RIN 0750–AG47

Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011–D039)

**AGENCY:** Defense Acquisition Regulations System, Department of Defense (DoD).

**ACTION:** Final rule.

78 Fed. Reg. 69273 (Nov. 18, 2013)
### Cyber Risks – DoD Rule

#### Are You DFAR’d?

- **Broad Reach of DFARS Rule**
  - All solicitations & contracts
  - Technical information everywhere
- **Mandatory Controls**
  - Comply – or else
  - PCO waiver: Can you get it?
- **Incident Reporting**
  - No safe harbor
  - Incident response team ready?
- **Subcontractor Flowdown**
  - Who reports what, where & to whom?

#### Noncompliance Risk?

**Too Soon to Tell but . . . . . .**

- Default Termination
- Out of Competitive Range
- Lost Awards & Protests

**What’s Next?**

- Prime/Sub Disputes
- Debarment (*e.g.*, L-3)
- FCA Claims (*e.g.*, PlastiLam)
Cyber Risks – SEC Scrutiny

SEC Scrutiny

SEC Standard

- Disclose material risks?

Impact

→ SEC scrutiny or actions

“Cyber risk management is a critical corporate responsibility. Federal securities law requires publicly traded companies to disclose ‘material’ risks and events, including cyber risks and network breaches. A review of past disclosures suggests that a significant number of companies are failing to meet these requirements.” [Senate Commerce News Release, May 12, 2011]

Disclosure Duty

Division of Corporation Finance
Securities and Exchange Commission
CF Disclosure Guidance: Topic No. 2 Cybersecurity
Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents

Disclosure Duties

• Risk of Cyber Incidents
• Prior Security Breaches
• Adequacy of Preventative Measures
Private Actions & Impact

**$20 Million Suit.** Countrywide’s lax “internal procedures” & security breach [Courthouse News, Apr. 5, 2010]

**B2B Disputes.** “VISA also removed the company from its list of approved processors.” [GAO, June 2012]


Shareholder Actions

“Delaware’s Court of Chancery ruled in the 1996 *Caremark* case that a director’s good faith duty includes a duty to attempt to ensure that a corporate information and reporting system exists and that failure to do so may render a director liable for losses caused by the illegal conduct of employees. The Delaware Supreme Court clarified this language in the 2006 *Stone v. Ritter* case – deciding that directors may be liable for the damages resulting from legal violations committed by the employees of a corporation, if directors fail to implement a reporting system or controls or fail to monitor such systems.”

Questions?

David Z. Bodenheimer
Crowell & Moring LLP
dbodenheimer@crowell.com
(202) 624-2713