

# Funds in Focus 2018:

## Private Investment Funds Annual Review Conference

FinTech: Investing in Digital Assets and  
Using Big Data

Jeff Neuburger, Jeremy Naylor,  
Stephen Mears, Rob Leonard, Mike  
Mavrides, Chris Wells

Proskauer»





FinTech: Investing in Digital Assets and Using Big Data  
Big Data and Hedge Funds:  
Current Legal and Compliance Issues

# Summary

---

## 1. Introduction

- Why are we here? Emergence of “Big Data” as an industry trend.
- Managers can acquire the data themselves and/or commission or otherwise acquire the data from third parties through a variety of different arrangements.
- Contracts relating to Big Data require special consideration.
- Violation of laws/agreements could result in civil issues and possibly trigger potential securities law violations.
- Not Expert Networks 2.0.

## 2. What is “Big Data?”

- Different types of data used by fund managers (e.g., consumer info, industry trends, satellite photos, etc.).

# Summary *(cont'd)*

---

## 3. How does one acquire “Big Data?”

- Describe the various techniques for acquiring the data (e.g., scraping, crawling, drones, etc.).

## 4. What are the key legal issues/concerns raised by the use of “Big Data”?

- An overview of the key legal issues and concerns implicated by the use of “Big Data.”
- Discuss insider trading and other securities law issues and concerns.

## 5. What are the key takeaways for fund managers?

- Discuss policies, procedures and practices.

## 6. Final Remarks/Questions

# Big Data: A Potential Kitchen Sink of Claims

- Breach of contract (e.g., website terms, EULA, API terms)
- CFAA (and equivalent state computer trespass law)
- Direct and contributory copyright infringement; DMCA
- Common law trespass; conversion
- Unfair competition
- Misappropriation

UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION	
CRAIGSLIST, INC., a Delaware corporation,	Case No. CV 12-03816 CRB
Plaintiff,	<b>FIRST AMENDED COMPLAINT FOR:</b>
v.	(1) Breach of Contract
3TAPS, INC., a Delaware corporation; PADMAPPER, INC., a Delaware corporation; DISCOVER HOME NETWORK, INC., a Delaware Corporation d/b/a LOVELY; BRIAN R. NIESSEN, an individual, and Does 1 through 25, inclusive,	(2) Trespass
Defendants.	(3) Misappropriation
	(4) Violations of the Computer Fraud and Abuse Act
	(5) Copyright Infringement
	(6) Contributory Copyright Infringement
	(7) Federal Trademark Infringement
	(8) Federal False Designation of Origin
	(9) Federal Dilution of a Famous Mark
	(10) Federal Cyberpiracy Prevention
	(11) California Trademark Infringement
	(12) Common Law Trademark Infringement
	(13) California Unfair Competition
	(14) California Comprehensive Computer Data Access and Fraud Act
	(15) Aiding and Abetting Trespass
	(16) Aiding and Abetting Misappropriation
	(17) Accounting
	<b>DEMAND FOR JURY TRIAL</b>

# Contract Issues

**WELCOME TO CRAIGSLIST.** We hope you find it useful. By accessing our servers, websites, or content therefrom (together, "CL"), you agree to these Terms of Use ("TOU"), last updated December 05, 2013.

**LICENSE.** If you are 18 or older, we grant you a limited, revocable, nonexclusive, nonassignable, nonsublicensable license to access CL in compliance with the TOU; unlicensed access is unauthorized. You agree not to license, distribute, make derivative works, display, sell, or "frame" content from CL, excluding content you create and sharing with friends/family. You grant us a perpetual, irrevocable, unlimited, worldwide, fully paid/sublicensable license to use, copy, perform, display, distribute, and make derivative works from content you post.

**USE.** You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly licensed by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, flagging, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited, as are misleading, unsolicited, unlawful, and/or spam postings/email. You agree not to collect users' personal and/or contact information ("PI").

**MODERATION.** You agree we may moderate CL access and use in our sole discretion, e.g. by blocking (e.g. IP addresses), filtering, deletion, delay, omission, verification, and/or access/account/license termination. You agree (1) not to bypass said moderation, (2) we are not liable for moderating, not moderating, or representations as to moderating, and (3) nothing we say or do waives our right to moderate, or not. All site rules, e.g. [cl.com/about/prohibited](http://cl.com/about/prohibited), are incorporated herein.

**SALES.** You authorize us to charge your account for [CL fees](#). Unless noted, fees are in US dollars; tax is additional. To the extent permitted by law, fees are nonrefundable, even for posts we remove. We may refuse purchases, which may place a hold on your account.

**DISCLAIMER.** MANY JURISDICTIONS HAVE LAWS PROTECTING CONSUMERS AND OTHER CONTRACT PARTIES, LIMITING THEIR ABILITY TO WAIVE CERTAIN RIGHTS AND RESPONSIBILITIES. WE RESPECT SUCH LAWS; NOTHING HEREIN SHALL WAIVE RIGHTS OR RESPONSIBILITIES THAT CANNOT BE WAIVED.

To the extent permitted by law, (1) we make no promise as to CL, its completeness, accuracy, availability, timeliness, propriety, security or reliability; (2) your access and use are at your own risk, and CL is provided

# Contract Issues

**WELCOME TO CRAIGSLIST.** We hope you find it useful. By accessing our servers, websites, or content therefrom (together, "CL"), you agree to these Terms of Use ("TOU"), last updated December 05, 2013.

**LICENSE.** If you are 18 or older, we grant you a limited, revocable, nonexclusive, nonassignable, nonsublicensable license to access CL in compliance with the TOU; unlicensed access is unauthorized. You agree not to license, distribute, make derivative works, display, sell, or "frame" content from CL, excluding content you create and sharing with friends/family. You grant us a perpetual, irrevocable, unlimited, worldwide, fully paid/sublicensable license to use, copy, perform, display, distribute, and make derivative works from content you post.

**USE.** You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly licensed by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, flagging, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited, as are misleading, unsolicited, unlawful, and/or spam postings/email. You agree not to collect users' personal and/or contact information ("PI").

**MODERATION.** You agree we may moderate CL access and use in our sole discretion, e.g. by blocking (e.g. IP addresses), deletion, delay, omission, verification, and/or access/account/license termination. You agree not to bypass said moderation, (2) we are not liable for moderating, not moderating, or removing content, and (3) nothing we say or do waives our right to moderate, or not. All site rules, [out/prohibited](#), are incorporated herein.

**SALES.** You agree to pay our account for [CL fees](#). Unless noted, fees are in US dollars; tax is additional. ~~CL fees are nonrefundable even for posts we remove. We may~~

**USE.** You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly licensed by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, flagging, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited, as are misleading, unsolicited, unlawful, and/or spam postings/email. You agree not to collect users' personal and/or contact information ("PI").



# Contract Issues

**WELCOME TO CRAIGSLIST.** We hope you find it useful. By accessing our servers, websites, or content therefrom (together, "CL"), you agree to these Terms of Use ("TOU"), last updated December 05, 2013.

**LICENSE.** If you are 18 or older, we grant you a limited, revocable, nonexclusive, nonassignable, nonsublicensable license to access CL in compliance with the TOU; unlicensed access is unauthorized. You agree not to license, distribute, make derivative works, display, sell, or "frame" content from CL, excluding content you create and sharing with friends/family. You grant us a perpetual, irrevocable, unlimited, worldwide, fully paid/sublicensable license to use, copy, perform, display, distribute, and make derivative works from content you post.

**USE.** You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly licensed by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited. Posting, sending, unsolicited, unlawful, and/or spam postings/email. You agree not to collect user information ("PI").

## Enforceable?

## Contract Issues

---

### Website “Terms of Use”

**WELCOME TO CRAIGSLIST.** We hope you find it useful. By accessing our servers, websites, or content therefrom (together, “CL”), you agree to these Terms of Use (“TOU”), last updated December 05, 2013.

**LICENSE.** If you are 18 or older, we grant you a limited, revocable, nonexclusive, nonassignable, nonsublicensable license to access CL in compliance with the TOU; unlicensed access is unauthorized. You agree not to license, distribute, make derivative works, display, sell, or “frame” content from CL, excluding content you create and sharing with friends/family. You grant us a perpetual, irrevocable, unlimited, worldwide, fully paid/sublicensable license to use, copy, perform, display, distribute, and make derivative works from content you post.

**USE.** You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly provided by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited. Unsolicited, unlawful, and/or spam postings/email. You agree not to

# Will the Site Owner Enforce?

## Contract Issues

---

### Website “Terms of Use”

**WELCOME TO CRAIGSLIST.** We hope you find it useful. By accessing our servers, websites, or content therefrom (together, “CL”), you agree to these Terms of Use (“TOU”), last updated December 05, 2013.

**LICENSE.** If you are 18 or older, we grant you a limited, revocable, nonexclusive, nonassignable, nonsublicensable license to access CL in compliance with the TOU; unlicensed access is unauthorized. You agree not to license, distribute, make derivative works, display, sell, or “frame” content from CL, excluding content you create and sharing with friends/family. You grant us a perpetual, irrevocable, unlimited, worldwide, fully paid/sublicensable license to use, copy, perform, display, distribute, and make derivative works from content you post.

**USE.** You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly provided by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited. Unsolicited, unlawful, and/or spam postings/email. You agree not to

**Craigslist, Inc. v RadPad, Inc., No.  
16-01856 (N.D. Cal. Final Judgment  
Apr. 13, 2017)**

# Mobile Phone Issues

---

- **Google Play (Android) Requirements:**

- You must be transparent in how you handle user data (e.g., information provided by a user, collected about a user, and collected about a user's use of the app or device), including by disclosing the collection, use, and sharing of the data, and you must limit use of the data to the description in the disclosure. If your app handles personal or sensitive user data, there are additional requirements..."

- **Apple Store Review Guidelines Recent Changes:**

**Former Section 5.1.2(ii)** (Color and bolding emphasis added):

- **Data** collected from apps may **not be used or shared** with third parties for purposes unrelated to improving the user experience or software/hardware performance connected to the app's functionality, or to serve advertising in compliance with the [Apple Developer Program License Agreement](#).
- **As of June, 2018, the concept is subsumed into Section 5.1.2(i):**
  - Unless otherwise permitted by law, you may not use, transmit, or share someone's **personal data** without first obtaining their permission. You must provide access to information about how and where the data will be used. **Data collected from apps may only be shared with third parties** to improve the app or serve advertising (in compliance with the [Apple Developer Program License Agreement](#)). Apps that share **user data** without user consent or otherwise complying with data privacy laws may be removed from sale and may result in your removal from the Apple Developer Program.
- **Unchanged (now in Section 5.1.2(ii) of App Store Review Guidelines:**
  - **Data** collected for one purpose may not be repurposed without further consent unless otherwise explicitly permitted by law.
- **Unchanged - Apple Developer Program Information**, Section 3.3.9: You and Your Applications ... may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising ... You may not use analytics software in Your Application to collect and send device data to a third party.

# Computer Fraud and Abuse Act

---

18 U.S.C. §1030 – Fraud and related activity in connection with computers

- Provides civil/criminal cause of action for access to a “protected computer” “without authorization or exceeding authorized access,” and obtaining information, causing damage or loss, or furthering a fraud, among other things.
- Many states have parallel or similar computer fraud statutes.
- Must show \$5,000 in damages.
- **Key Question:** What is exceeding authorized access? Is breach of terms of use enough?

# Scraping of “Public” Website Data

---

*hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F.Supp.3d 1099 (N.D. Cal. 2017)

- Involves LinkedIn's challenge to hiQ's scraping of LinkedIn public profile data.
- **Key question:** Whether, by continuing to access public LinkedIn profiles after LinkedIn explicitly revoked permission to do so, hiQ has "accessed a computer without authorization" within the meaning of the CFAA.
- Court granted injunctive relief against LinkedIn's blocking of hiQ's scraping activities.
- Lower court expressed "serious doubt" as to whether LinkedIn's revocation of permission to access the *public* portions of its site renders hiQ's access "without authorization."
  - “[I]n the context of a publicly viewable web page open to all on the Internet, the 'plainness' of the meaning of 'access' 'without authorization' is less obvious. Context matters.”
- **On appeal to the Ninth Circuit.** Oral arguments were held Mar. 15, 2018.

# Scraping of “Public” Website Data

---

## ***Sandvig v. Sessions, No. 16-1368 (D.D.C. Mar. 30, 2018)***

- A group of professors and a media organization were conducting research into whether the use of algorithms by various housing and employment websites to automate decisions produces discriminatory effects.
- Brought a constitutional challenge alleging that the potential threat of criminal prosecution under the CFAA for accessing a website “without authorization” violates their First Amendment rights.
- The court stated that much of the plaintiff’s planned scraping behaviors – scraping of public website data, publishing of data stemming from such research and the use of bots to access and interact with a public website – were not CFAA violations.
- Scraping may be a violation of the ToS, but is not “exceeding authorized access.”

# Scraping of “Private” Websites

---

## *Ticketmaster L.L.C. v. Prestige Entm’t, Inc., No. 17-07232 (C.D. Cal. Jan. 31, 2018)*

- Defendant ticket brokers used bots and dummy accounts to navigate Ticketmaster’s website and mobile app to purchase large quantities of tickets to popular events.
- As part of the ticket buying process, users must agree to Ticketmaster’s terms of use before they can view and use Ticketmaster’s website and mobile app.
- CFAA claim: Following *Power Ventures*, the court looked to the revocation of access and how it was communicated.
  - Ticketmaster contended that defendants lacked or exceeded their authorization by violating its terms, even after it sent defendants a cease and desist letter outlining the alleged violations.
  - In dismissing the claim, with leave to amend, the court found that Ticketmaster’s cease and desist letter had “not shown that it rescinded permission from Defendants to use its website.”
  - Court also noted that Ticketmaster’s Complaint was “wholly devoid of any allegations suggesting that Ticketmaster took steps to prevent Defendants from future access.”

# Scraping of “Private” Websites

---

## *Ticketmaster L.L.C. v. Prestige Entm’t, No. 17-07232 (C.D. Cal. May 29, 2018)*

- Ticketmaster filed an (amended) complaint and defendant moved to dismiss.
- **CFAA:** Ticketmaster argued that each use of a bot to purchase a ticket was a use in excess of authorization because a C&D Letter explicitly prohibited defendants from using bots to access the site.
- Defendants countered that they did no more than violate the ToU, and as such cannot provide the basis for CFAA liability.
- Court allowed CFAA claim to go forward as it is the violation of the terms of the C&D Letter, not of Ticketmaster's terms, on which the court bases its finding of a well-pled CFAA claim.
  - “The *Power Ventures* court required something ‘more’ than mere violation of a website owner's terms of use to impose liability under the CFAA, and the Letter satisfies that requirement.”

# Scraping of “Private” Websites

---

## ***BidPrime, LLC v. SmartProcure, Inc.*, No. 18-478 (W.D. Tex. June 18, 2018)**

- Texas district court denied a bid from a web service for a TRO to enjoin a competitor that allegedly scraped a large amount of proprietary data from its closed site via several user accounts.
- While tempting to draw a general legal conclusion about the permissibility of scraping from this decision, the decision was in fact based on the judgement of the court that scraping was unlikely to continue during the pendency of the litigation.
- See also *Lemonade, Inc. v. One Versicherung AG*, No. 18-5368 (S.D.N.Y. Complaint filed June 14, 2018) (insurer lodged CFAA and contract claims against a competitor for allegedly created fake accounts to access the insurer’s app to extract data on pricing and claim procedures).

# Scraping of “Private” Websites

---

## **Alan Ross Mach. Corp. v. Machinio Corp., No. 17-3569 (N.D. Ill. July 9, 2018)**

- Plaintiff alleged its competitor Machinio Corp. scraped sales listings of industrial machines from plaintiff’s website and listed such data on the Machinio site.
- Alan Ross alleged that it “expressly demanded that Machinio not scrape its website.”
- Illinois district court dismissed claims, with leave to amend, relating to a competitor’s alleged scraping of sales listings from a company’s website for use on its own site.
- The court dismissed a CFAA claim that the defendant accessed the plaintiff’s servers “without authorization,” finding that the plaintiff failed to plead with specificity any damage or loss related to the scraping. In the court’s view, the “mere copying of electronic information from a computer system is not enough to satisfy the CFAA’s damage requirement.”
- Court also dismissed plaintiff’s breach of contract claims, concluding that defendant did not have notice of the plaintiff’s website terms and conditions based upon an unenforceable browsewrap agreement.

# Computer Fraud and Abuse Act

---

- Did you violate the terms of use?
- Did you get a cease and desist letter?
- Are you circumventing technical measures to block access?
  - Did you conceal who you are by manipulating the “User-Agent” in your http call?
  - Did you check the robots.txt file for the site?
  - Did you pay any attention to what is in it?
  - Did you manipulate IP addresses?
  - Did you take any other actions to hide access?

# U.S. Privacy and Data Security Law

---

- A sector-by-sector approach:
  - Medical information
  - Financial information
  - Sensitive personal information
  - Children's privacy
  - School records
  - Communications
  - Computers
  - Cable subscriber information
  - GPS tracking

# Electronic Communications Privacy Act and the Stored Communications Act

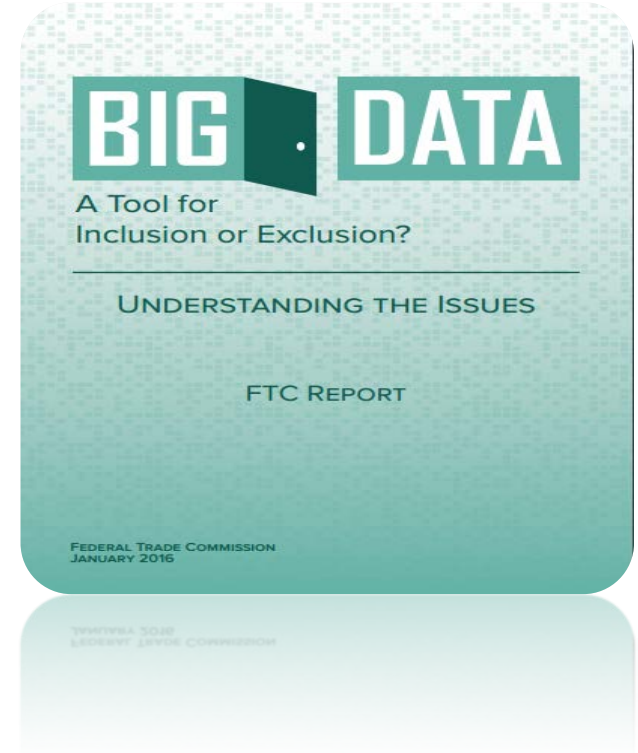
---

18 U.S.C. §2511; 18 U.S.C. §2701

- The ECPA provides a private right of action against any person who intentionally intercepts any "wire, oral, or electronic communications."
- The Stored Communications Act prohibits certain unauthorized access to stored communications and records.
- The ECPA allows for "*use*" and "*disclosure*" liability.
  - Liability extends to intentional use or disclosure of illegal intercepted communications, where one knows the information used or disclosed came from an intercepted communication and had sufficient facts that such interception was prohibited.

# FTC 2016 Big Data Report

The agency advises companies using big data to consider whether they are violating any material promises to consumers involving data sharing, consumer choice or data security, or whether companies have otherwise failed to disclose material information to consumers. Such violations of privacy promises have formed the basis of multiple FTC privacy-related enforcement actions in recent years.



# Avoidance of Personally Identifiable Information (PII)

---

- De-identified Information (NIST Definition): “Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.”
- Anonymized Information (NIST Definition): “Previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists.”

# Copyright

---

17 U.S.C. §106; 17 U.S.C. §504

- In certain circumstances, automated data collection may infringe upon a site owner's copyright.
- If web scraping leads to the reproduction of any copyrighted content, such activity may give rise to a claim for copyright infringement.
- Special considerations when it comes to User Generated Content Issues.
- Circumvention of technological control measures, such as CAPTCHA “I am not a robot” measures to block automated access, could create the basis for liability under the Digital Millennium Copyright Act (“DMCA”).

# Trespass

---

- Excessive automated data collection can interfere with the performance of a site.
- To the extent a site crashes, an end-user experiences delays, or a site's operational capacity is otherwise burdened, the data collector may be deemed to have interfered with the site owner's use of its tangible property.
- This could constitute a trespass to chattels.

# Data Collection & Drones

---

- FAA unmanned aircraft regulations (a/k/a drone regulations) for recreational purposes invalidated (*Taylor v. Huerta*, No. 15-1495 (D.C. Cir. May 19, 2017)).
- Commercial regulations remain in effect and require operators to obtain a drone license, and report the aircraft's intended use, time or number of flights, and area of operation (e.g., away from sensitive areas), among other things.
- There are also state and local laws re: drone usage, with some laws prohibiting surveillance of critical infrastructure or flying over a person's private property where a person may reasonably expect to be safe from observation.

# Data Collection & Drones

---

- The National Telecommunications and Information Administration released best privacy practices for drones:
  - 1) inform others of your use of drones;
  - 2) show care when operating drones and storing data;
  - 3) limit use and sharing of covered data;
  - 4) secure covered data; and
  - 5) monitor and comply with federal, state and local drone laws.

---

## Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

---

Consensus, Stakeholder-Drafted  
Best Practices Created  
in the NTIA-Convened  
Multistakeholder Process

May 18, 2016

# MNPI – Deceptive Conduct

---

- DOJ – Use of SOX securities fraud statute 18 U.S.C. 1348
  - Section 1348 applied to insider trading (e.g., *U.S. v. Blaszczyk*).
    - (1) a scheme or artifice to defraud;
    - (2) fraudulent intent; and
    - (3) a nexus with a security.
  - Typical elements of 10b-5 insider trading are not applicable.
    - No breach of fiduciary duty, personal benefit, or personal knowledge of the benefit.
- July 2018: *U.S. v. Korchevsky* criminal verdict
  - Mail fraud, wire fraud and securities fraud under Section 1348.

# MNPI – Deceptive Conduct

---

- SEC/Civil – 10b-5 “scheme” liability
  - *SEC v. Dubovoy* (August 2015)

SEC and DOJ charged dozens of traders in scheme to trade on hacked news releases.

- Deceptive conduct included hiding intrusions by using proxy servers to mask their identities and by posing as employees.
- Charges: mail & wire fraud, securities fraud, conspiracy, etc.
- Same scheme charged criminally in *Korchevsky*.
- 2d Cir: misrepresenting ones identity in order to gain access is plainly “deceptive” under 10b-5.

- Advisers Act Rule 204A

- Failure to establish, maintain, and enforce policies and procedures reasonably designed to prevent the misuse of MNPI.
- Recent cases focus on inadequate measures to “enforce” policies and procedures, in light of particularized risks.

# Insider Trading: Computer Hacking

---

- ***SEC v. Hong*** (December 2016)
  - Chinese traders charged with hacking into law firm computer networks.
    - Deceptive conduct included installing malware, stealing passwords, electronically impersonating IT employee.
- Liability when access involved deception/breach of duty

# Insider Trading: Misappropriation Theory

---

- Misappropriation theory prohibits:
  - Any person or entity from trading
  - On basis of material, nonpublic information
  - That has been ***misappropriated*** from a party
  - To whom person owes a duty, or whom he/she deceives.
- Liability requires a duty of trust or confidence
  - Duty runs to ***source of info***, not to issuer of securities traded.
- Under **Rule 10b5-2**, person has a duty of trust or confidence:
  - When a person **agrees to keep info confidential**;
  - There is history, pattern, or practice of sharing confidences; or
  - Information from his/her spouse, parent, child, or sibling.

# Misappropriation Theory: Two Examples

---

- ***U.S. v. Carpenter*** (2d Cir. 1986)
  - *WSJ* columnist provided advance information about contents of his “Heard on the Street” column.
    - Tippees traded on information, as did columnist.
  - Advance disclosure violated *WSJ* policy that deemed all news materials to be company property and confidential.
  - Columnist was convicted of having misappropriated *WSJ*’s property in breach of his duty to his employer.
    - But court noted that *WSJ* itself might have been able to use undisclosed info from “Heard on the Street,” because *WSJ* owned the information and would not have breached duty to anyone.

# Misappropriation Theory: Two Examples

---

- ***SEC v. Huang*** (E.D. Pa. 2016), *aff'd* (3d Cir. 2017)
  - Data analyst for Capital One downloaded and analyzed data re: retail purchases made with Capital One credit cards.
    - He used this info to predict revenues of retailers who used Capital One cards, and he then traded retailers' stocks.
  - Use of info violated Capital One's confidentiality policies.
  - Found liable for insider trading on misappropriation theory.
    - Breach of duty to his employer.
  - Courts concluded that jury could have found credit-card info material even though Capital One card usage represented an average of only 2.4% of retailers' revenues.

# Insider Trading: Computer Hacking

---

- **SEC v. Dorozhko** (2d Cir. 2009)
  - Ukrainian programmer hacked into IR company's computer and obtained advance info about earnings reports.
    - Hacker traded on MNPI obtained through hack.
  - 2d Circuit held liability depended on whether hack was “deceptive.”
    - “[M]isrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly ‘deceptive’ within the ordinary meaning of the word.”
    - If deception occurred: potential insider-trading liability.
  - If hacker merely exploited weakness in electronic code to gain unauthorized access: perhaps theft, but not “deception.”

# Accessing Nonpublic Information

---

- Insider-trading liability will depend on whether method of access to MNPI involved breach of duty or deception.
  - Was access to information obtained legitimately?
  - Remember *Dorozhko*, the Ukrainian hacker:
    - Insider-trading liability depends on whether access was “deceptive.”
      - If you *misrepresent* your ID to gain access to computer system, deception occurred – potential insider-trading liability.
      - If you merely exploit weakness in electronic code to gain unauthorized access: perhaps no deception involved.
        - But might be theft.

# Accessing Nonpublic Information (*cont'd*)

---

- Whether access involved deception/breach of duty (*cont'd*)
  - Violation of website's Terms of Use
    - Is it deception?
      - Will evasions of technological restrictions be deceptive?
        - If user misled website by masking or rotating its IP address, deception involved?
    - Is it a breach of duty?
      - If user agrees to abide by use restrictions, but does not do so?
  - Violation of contract with owner of information
    - Deception or breach of duty if user pays owner for access to information, but uses information in ways or for purposes that contract does not allow?

# Contracts with Source/Owner of MNPI

---

- Contract between would-be user of MNPI and owner of information
  - If usage is in accordance with contract terms/limitations, perhaps no misappropriation, because owner of MNPI has not been deceived/misled.
    - Remember *Carpenter*: 2d Cir. noted that *WSJ* or its parent (Dow Jones) might have been able to trade on advance info from “Heard on the Street,” because they owned the information – no breach of duty.
      - Perhaps Capital One could have traded on credit-card information?
  - But does owner of info have duty to anyone?
    - Any duty to its own customers to keep information confidential and not use it except for certain purposes?
    - If so, does a person/company that makes contract with owner know about this duty and about any breach by owner?

# Contracts with Source/Owner of MNPI

---

- Contract with owner of information (*cont'd*)
  - Even if owner of info does not breach any duty, contracting party might have other risk of liability even if no insider trading.
    - NY's Martin Act authorizes NY AG to sue based on unfairness.
      - Information disparity suffices; breach of duty/fraud not needed.
    - NY AG has threatened to use Martin Act re insider trading.
      - Thomson Reuters/U. Mich. settlement: Thomson agreed to stop selling to priority subscribers early access to consumer-confidence survey.
      - 18 large B/Ds agreed to stop responding to buy-side firms' surveys seeking analyst sentiment.
      - PR Newswire, Business Wire, and Marketwired agreed to require subscribers to certify they would not do high-frequency trading with info received from outlets' direct data feeds.

# Contracts with Source/Owner of Info

---

- Contract with owner of information (*cont'd*)
  - Also need to consider EU Market Abuse Regulation.
    - EU regulation can apply to transactions anywhere in world.
    - Test is whether security is *admitted for trading on EU markets*.
    - If security is traded in EU, place of transaction involving MNPI is irrelevant.
      - If U.S. trader uses MNPI in transaction with U.S. counterparty on U.S. market, EU Reg applies if security is also traded in EU.

# Contracts with Source/Owner of Info

---

- Contract with owner of information (*cont'd*)
  - EU rules on insider trading differ radically from U.S. rules
    - EU prohibits use of material, nonpublic information.
      - Applies to anyone who knew or should have known that material information was nonpublic.
    - Defenses available in U.S. are not available in EU.
      - Irrelevant whether discloser had duty not to disclose.
      - Irrelevant whether discloser received a personal benefit.
      - Irrelevant whether recipient owed duty to discloser not to use or disclose the information.
    - Under EU rules, if you know or should have known you have MNPI, you cannot use it – period.

# Acquiring Data from Third Parties

---

Can I reduce my risk  
by hiring a third party  
to do this for me?

# Acquiring Data from Third Parties – Diligence

---

- What might be acceptable risk to the vendor may not be acceptable risk for you.
- Technology and business models are way ahead of the law; creativity is high; “safe” practice standards do not exist and the urge to differentiate and add value is pressing.
- Contractual protection may not be enough to shield one from liability. It certainly is not enough to shield from litigation and adverse publicity.

# Spitzer Settles With Datran For \$1.1M

by **Wendy Davis** @wendyndavis, March 14, 2006

E-mail marketing company Datran Media has agreed to pay \$1.1 million to close an investigation by New York State Attorney General Eliot Spitzer into what his office called the largest breach of privacy in Internet history.

The investigation found that Datran obtained e-mail addresses and other information about consumers from companies that had promised on their Web sites not to share such information.

With the settlement, Spitzer's office promised to stop investigating the e-mail marketing company. For its part, Datran agreed to pay \$750,000 in penalties, \$300,000 disgorgement and \$50,000 costs, destroy consumer information that was wrongly collected, and appoint a chief privacy officer.



# Acquiring Data from Third Parties – Diligence

---

- **Trend, led by the FTC, for expanded vendor diligence and oversight.**
- **The “WSJ” Test.**
- **Legal “Flow Through” Liability.**
- **Agency Relationships.**

# Acquiring Data from Third Parties

---

- The Due Diligence Process:
  - Ask the questions in writing; get the answers in writing.
  - Document who is providing the answers and why it is reasonable to accept their responses.
  - Follow up; if it doesn't sound right, it probably isn't.
  - Spot-check the data.
  - Don't use the data other than as provided for in the contract.

# Acquiring Data from Third Parties

---

- The Due Diligence Process (*cont'd*):
- Get appropriate contractual reps/warranties/indemnities.
  - Make sure there is at least annual recertification.
    - Consider other triggers for recertification as well: Change of control, MAE, etc.
  - Avoid relying on the vendor's legal analysis.

# Fundamental Questions

---

- Who is the vendor? Is it credible, established, respected?
- What are the vendor's data sources?
- Where is the data coming from? Government or private sources?
- What is the nature of the data? What techniques does the vendor use?
- PII? Child PII? Sensitive Information?
- Any MNPI or other “confidential” information? (Spot-check!)
- Is the vendor collecting the same data for anybody else?

# Fundamental Questions

---

- Has there been any litigation involving the vendor or its sources?
- How does the vendor provide the data? Is the vendor a collector, packager, analyzer, aggregator?
- Does the vendor have the right to provide the data to you?  
Consider requesting documentation and indemnity.
- If using drones, does the vendor employ or contract with drone operators possessing proper commercial licenses acting in compliance with state and federal laws and NTIA best practices?

# Fundamental Questions

---

- Does the vendor spider? If so:
  - Do the targeted websites have restrictive terms of use? Does the vendor check regularly?
  - Does the vendor use technology to simulate the creation of any user accounts?
  - Does the vendor circumvent any “captchas” or similar technologies?
  - Does the vendor respect the “robots.txt” parameters?
  - Does the vendor identify its “User-Agent” in the site logs?
  - How does the vendor structure IP addresses for spidering?
  - Does the vendor throttle/pause/alternate times to simulate human interaction?

# Closing Thoughts

---

- Create and follow policies.
- Be clear with all about MNPI – you don't want it!
- Document your procedures.
- Negotiate appropriate contractual provisions.
- Vendors: Certify, recertify and recertify again!
- Stay aware of evolving law!



## FinTech: Investing in Digital Assets and Using Big Data

### Recent CFTC and SEC Developments

# CFTC Developments

---

- Digital currencies are commodities subject to CFTC oversight.
  - Confirmed by courts in *CFTC v. McDonnell* and *CFTC v. Crater*.
  - Subject to CFTC anti-fraud/anti-manipulation jurisdiction.
  - Futures or forward contracts in digital currencies unlawful unless traded on regulated futures exchange.
- NFA requires registered CPOs and CTAs to include specific disclosures regarding cryptocurrency investments in disclosure documents (NFA Notice 1-18-13).
- NFA requires registered CPOs and CTAs to report digital currency holdings in annual questionnaire and fund reports (NFA Notice 1-17-28).

# SEC Developments

---

- SEC authority over digital “tokens” (ICOs) confirmed by courts:
  - *United States v Zaslavskiy*, E.D.N.Y. No. 1:170-cr-00647
  - *Crypto Asset Management, LP*, Cease and Desist Order
  - *SEC v. Blockvest, LLC*, S.D. Cal. No. 18-CV-2287-GPC
- But “pure” digital currency like Bitcoin or Ethereum is not a security per *Howey* Test, because expectation of profit is no longer “derived primarily from the efforts of others.”
  - That said, private fund managers should tread lightly.

# Key Consequences

---

- Custody Rule applies to digital tokens (i.e., “as securities”).
  - Tokens must be held by bank or broker-dealer.
  - Cryptocurrencies?
- Valuation issues:
  - Digital assets often trade at different prices on different markets and digital exchanges have at times closed or suspended trading.
  - It will be critical to have strong valuation "practices" that are in line with disclosures to investors and supported by robust policies and procedures that are consistently applied.

# Key Consequences

---

- Employees must report personal trading in digital tokens (i.e., “as securities”).
  - Up to manager whether cryptocurrency trades must be reported.
- Both SEC and CFTC watching very closely.
  - Cryptocurrencies and ICOs were included in OCIE's 2018 exam priorities and are the subject of a sweep exam.



# FinTech: Investing in Digital Assets and Using Big Data

## Digital Assets – Fund LPA Considerations

# Digital Assets – Fund LPA Considerations

---

- Purpose Clause
- Investment Limitations
  - Public investments, Non-US investments.
- Crypto Asset Percentage Limits
  - All Crypto Assets, Bitcoin vs tokens.
- Conflict Provisions
  - Overlapping investments with other funds or sponsor personnel.
- Treatment as “Portfolio Securities”
  - Including for carried interest calculations.
- Distributions in Kind
- Valuation Provisions
- Tax
  - UBTI/ECI undertakings.



# FinTech: Investing in Digital Assets and Using Big Data

## Digital Assets – Tax Issues

# Digital Assets – Tax Issues

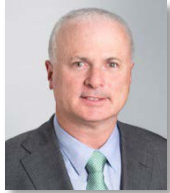
---

- General tax treatment
  - Security? Commodity? Currency?
  - IRS Notice 2014-21 – Property under general tax principles
  - Like kind exchanges? Not after tax reform
  - Trading consequences
    - Mark to market?
    - Non-US investors? ECI? Trading safe harbor apply?
    - Tax-Exempt investors? UBTI?
- Tax issues for funds investing in companies issuing tokens
  - Treatment of distributions of tokens/crypto
  - Subpart F issues for investors in foreign token issuers
- Contributions and distributions of digital assets to and from funds
  - Taxable? Tax-free?
- Information reporting – 1099; FBAR; Foreign asset reporting (Form 8938)

# Contacts

---

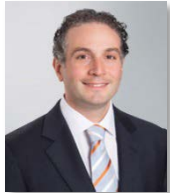
## Hedge Funds



**Robert Leonard**

212-969-3355

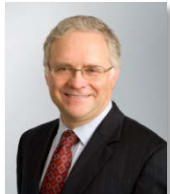
[rleonard@proskauer.com](mailto:rleonard@proskauer.com)



**Michael Mavrides**

212-969-3670

[mmavrides@proskauer.com](mailto:mmavrides@proskauer.com)



**Christopher Wells**

212-969-3600

[cwells@proskauer.com](mailto:cwells@proskauer.com)

## Private Funds

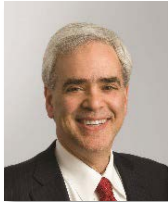


**Stephen Mears**

617-526-9775

[smears@proskauer.com](mailto:smears@proskauer.com)

## Technology, Media & Telecommunications



**Jeffrey Neuburger**

212-969-3075

[jneuburger@proskauer.com](mailto:jneuburger@proskauer.com)

## Tax



**Jeremy Naylor**

212-969-3375

[jnaylor@proskauer.com](mailto:jnaylor@proskauer.com)

# Funds in Focus 2018: Private Investment Funds Annual Review Conference



The information provided in this slide presentation is not, is not intended to be, and shall not be construed to be, either the provision of legal advice or an offer to provide legal services, nor does it necessarily reflect the opinions of the firm, our lawyers or our clients. No client-lawyer relationship between you and the firm is or may be created by your access to or use of this presentation or any information contained on them. Rather, the content is intended as a general overview of the subject matter covered. Proskauer Rose LLP (Proskauer) is not obligated to provide updates on the information presented herein. Those viewing this presentation are encouraged to seek direct counsel on legal questions. © Proskauer Rose LLP. All Rights Reserved.

