Panelists

Jaye S. Campbell
Deputy General Counsel – Head of Litigation
CoStar Group
jscampbell@costar.com
202-623-5257

Nicholas J. Boyle
Partner
Williams & Connolly
nboyle@wc.com
202-434-5343

David Randall J. Riskin
Partner
Williams & Connolly
driskin@wc.com
202-434-5789
Agenda

1. Introduction to CoStar Group
2. CoStar’s Digital Asset Theft Problem
3. In-house Strategies for Digital Asset Protection
4. Pre-litigation Case Studies
5. Competitor Litigation Case Study - Xceligent
6. User-Theft Case Study – Database-Fraud Litigation
7. Conclusion/Q&A
40+ Million Monthly Visitors to CoStar Websites
Millions of brokers, owners, tenants and others search for listings on CoStar’s marketplaces every day.
Banks, investors and owners use our information, analytics and forecasting tools to inform trillions of dollars of transactions.
Millions of Americans find their next home on Apartments.com™
Hundreds of retailers use our tools to manage billions of dollars in rent payments.
Government agencies at the federal, state and local levels use our data, analytics and indices
3,500+ Employees
CoStar to bring 730 jobs to new HQ in Richmond

Health law’s premiums set to rise sharply

HHS predicts average 25% jump before subsidies

BY RICARDO ALONSO-ZALDIVAR
The Associated Press

WASHINGTON — Premiums will go up sharply next year under President Barack Obama’s health care law, and many consumers will be down to just one insurer, the ad-versary involving the Affordable Care Act, also known as Obamacare, shortly before the presidential election.

Before taxpayer-provided subsidies, premiums for a midlevel benchmark plan will increase an average of 25 percent across the 39 states, including Virginia, served by the federally run online market, according to a report from the Department of Health and Human Ser-
Research Phone Interviews

12,251,837
FIELD RESEARCH

200 VEHICLES

4,000,000+ Buildings VISITED
Theft Issues Confronting CoStar

Competitor Theft:

Competitors seek to “build” competing databases and marketplaces by copying CoStar content or inducing CoStar subscribers to share CoStar content.

User Theft (Password Sharing):

Individuals and entities that do not subscribe to CoStar find ways to get access.
CoStar’s Digital Asset Protection Checklist

1. Register photos with the Copyright Office
2. Display binding terms of use on all websites
3. Deploy cutting edge digital content protection technologies
4. Attempt to stop theft by increasing security
5. Build comprehensive record of theft
6. Employ a theft team to monitor product usage and website traffic and to resolve confirmed instances of theft
7. Litigate when theft cannot be amicably remediated
Copyright Registration

• The Copyright Act permits the owner of a work to register the work with the Copyright Office

• Photos can be bulk registered

• Statutory damages are available for registered works:
  • Up to $150,000 per work infringed for willful infringement
  • Attorneys’ fees
  • Copyright is a strict liability tort; few defenses

• Not all content is protected by U.S. copyright law
Terms of Use

• The more the user must interact with the TOU, the more likely they are to be enforceable.
Leverage Technology

• Monitor and block excessive searching, page views and time in product

• Block countries from which normal website or product usage would not originate

• Block suspicious IP addresses, e.g. those associated with data mining, malicious web activity, or competitors

• Build real-time alerting based on suspicious website or product activity

• Alter the user experience based on alerts
Staff Appropriately – Theft Team

• Analysts, data scientists and investigators
• Monitor website and product usage for anomalies
• Immediate blocking of suspicious activity and notice
• Live call by investigator empowered with comprehensive electronic records
• Strong internal relationships with IT-Security and Product Development
Case Study 1: Technology + Theft Team

Legit CoStar credentials are issued to Heather of Company A

1. Heather’s account triggers a “bumpout” alert
2. Heather’s account has suspiciously named devices:

<table>
<thead>
<tr>
<th>Device</th>
<th># Activations</th>
<th>% Used</th>
<th>Last Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mike.</td>
<td>1</td>
<td>61.82</td>
<td>10/9/2018 2:40:59 PM</td>
</tr>
<tr>
<td>Laptop 1</td>
<td>1</td>
<td>16.36</td>
<td>10/4/2018 9:56:11 PM</td>
</tr>
<tr>
<td>Andrew</td>
<td>2</td>
<td>16.36</td>
<td>10/3/2018 5:57:36 PM</td>
</tr>
<tr>
<td>Heather’s Work Computer</td>
<td>1</td>
<td>3.64</td>
<td>9/19/2018 4:58:37 PM</td>
</tr>
<tr>
<td>Laptop</td>
<td>1</td>
<td>1.82</td>
<td>9/10/2018 10:41:49 AM</td>
</tr>
</tbody>
</table>
Heather’s Security Mode is Elevated to Facial

- Heather and unauthorized users are locked out and unable to access

- Company B signs up for CoStar subscription
Case Study 2: Technology + Theft Team

Legit CoStar credentials are issued to Lawyer V. at the V. Law Firm

1. Lawyer’s account triggers a suspicious mobile phone number alert

2. SMS code for Lawyer’s account is being sent to mobile phone associated with Tim G. of G & Co.
Lawyer V’s Security Mode is Elevated to Facial

Tim G attempts to access Lawyer V’s account (in a disguise) → Tim G’s identity confirmed through public sources → G & Co. brokerage signs up for CoStar
CoStar Litigates When Necessary

Recent judgments in CoStar’s favor include damages up to $14,000/image and future infringement payments of between $10,000 and $50,000 per image per day.

- CoStar v. RealMassive (W.D. Tex. 2015)
- CoStar v. ApartmentHunters (C.D. Cal. 2015)
Case Study 3: Litigation Against Xceligent

• Xceligent, based in Kansas City, was one of CoStar’s largest direct competitors

• Like CoStar, Xceligent offered a subscription database and a CRE marketplace

• Xceligent’s ultimate majority owner was a publicly traded company in London
The Genesis: A Whistleblower

• Theft Team swings into action
  • Traffic analysis / IP log review = The Philippines
  • Public information searches / LinkedIn = Xceligent
  • Competitor website review …
CoStar Built a Record of Xceligent’s Theft

~9,000 COSTAR COPYRIGHTED PHOTOS found in preliminary review of Xceligent’s public website

3.8 million PAGE VIEWS on CoStar’s Websites

800,000+ PROPERTIES Accessed on CoStar’s Websites

10+ million HITS to CoStar’s Websites
The Record Showed Notice and Sustained Improper Access

Access Denied

You are in breach of the binding LoopNet Terms and are blocked from accessing LoopNet. By continuing to access LoopNet or accessing after the block has expired, you are reaffirming your agreement to the LoopNet Terms. Users who do not comply with these Terms are not authorized to access LoopNet.

600+ times notified that they were in breach of LoopNet’s terms and what they were doing was ILLEGAL

45,000+ new requests for information after receiving notice of their breach
How Did Xceligent Try to Cover Its Tracks?
By Outsourcing the Theft
And Seeking to Circumvent CoStar’s Digital Security

• Xceligent and its agents in the Philippines and India circumvented CoStar’s blocking software using:
  – TOR browsers
  – Proxy servers
  – VPNs
  – IP address rotation
Legal Goals Checklist

- **Goal #1: Protect the IP.** Prevent future infringement and further dissemination of CoStar content.

- **Goal #2: Protect the Evidence.** Build a strong case despite circumvention of security, potential destruction of evidence, and fake or non-existent record keeping by the adversaries.

- **Goal #3: Hold the Violators Accountable.** Hold Xceligent and its foreign contractors accountable.
**Ex Parte Civil Seizure Orders**

- Although uncommon in the U.S., many countries permit plaintiffs to apply for *ex parte* civil seizure orders to protect evidence.
- Generally requires an evidentiary hearing without notice to adversary.
- Legal standard is high, but if met this is an extremely effective tool at preserving evidence of infringement.
Three Lawsuits, Three Countries

December 6, 2016
File for *ex parte* civil seizure against Xceligent agent in Manila

December 7, 2016
*Ex parte* civil seizure order granted in Manila

December 7, 2016
File for *ex parte* civil seizure against Xceligent agent in Mumbai

December 9, 2016
*Ex parte* civil seizure order granted in Mumbai

December 12, 2016

7:35PM Eastern
Sheriff in Laoag City and CoStar team begin seizure

9:00AM Eastern
Seizure begins in Mumbai

10:35PM Eastern
Complaint filed against Xceligent in W.D. Mo.

To be successful, the timing had to work just right.
Executing the Seizure Order in The Philippines

- 2 planes.
- 4 trucks.
- **Large team**: court commissioners, sheriffs, lawyers, forensic experts, corporate rep, security personnel.
Evidence Seized in The Philippines

• 262 computers.
• 34 terabytes of data.
• 6 million documents.
• 1.8 million images.
The Seized Evidence Was Devastating

• Screenshots of Avion employees *in the act* of circumventing CoStar security and copying content from CoStar websites.

• Skype logs documenting Xceligent’s instructions to Avion on *how* to circumvent CoStar’s digital security.

• E-mails from Xceligent managers *directing* foreign researchers to steal CoStar content.

• Significant evidence of other wrongdoing.
Screenshots Show the Xceligent M.O.: Copy from CoStar

- Open Xceligent’s backend system
- Google address using the term “LoopNet”
- Receive Access Denied message
- Access LoopNet through other methods, KProxy
- Update Xceligent System with CoStar content
Xceligent Researchers Caught in the Act

Town West Center, Indianapolis, IN 46254 – being added to CDX

Town West Plaza, Indianapolis, IN 46254 – viewed and took a screenshot on LoopNet
Chat Logs Show Xceligent Managers Directing the Circumvention of CoStar Security

“Guys you can use TOR browser to access Loop[N]et…”
– Xceligent’s Leslie Houston to Avion

“Good Morning [sir,] I believe that Brent [Hansen, an Xceligent manager] sent you sir an email regarding a software that shall be used by a couple of our agents in accessing [L]oop[N]et. . . . If you have the copy sir if it would be possible to forward it to the ITs. Thank you sir and have a great morning.”
– Avion to Xceligent’s Leslie Houston
Xceligent Faked Records to Hide Its Copying of Data From LoopNet

Auditor Notes
When copying listing notes from Loopnet, please rephrase it.

Lease Term of 36 months.

We cannot use the term "Loopnet" in the verification notes.

No marketing website added.

*marketing web: www.svn.com/find-properties/?propertyid=82106-lease

*Please revise verification notes (do not mention "loopnet" as much as possible, if the loopnet link has been sent through email, you can use "per email" as your reference and/or for google searches, you can use "third party source")

*add lease terms: 36 months (listing tab)

*add Zoning Code: C-3
Xceligent Cropped Out the CoStar Watermark

Example of image editing process: Cropping Tool
And Even Replaced CoStar’s Watermark with Its Own

CoStar logo to the right of the tree.

The image is cropped precisely to exclude only the original logo. CommercialSearch logo placed to the left of the tree.
The Seized Evidence Led to a Breakthrough

- Evidence led to U.S.-based affiliate of Indian contractor (MaxVal) known as RE BackOffice, Inc. (“REBO”).

- CoStar subpoenaed REBO for documents and took a third-party deposition in which it admitted misappropriating CoStar’s IP.

- Based on these admissions CoStar filed suit against REBO.
“[A]t Xceligent’s direction, the REBO/MaxVal operations team . . . circumvent[ed] CoStar’s security and thereby hack[ed] into CoStar’s sites in order to populate the Xceligent databases.”
Judgment Was Entered for Conspiring with Xceligent

**Holding:** REBO infringed CoStar’s copyrights and conspired with X to violate the CFAA and engage in unfair competition by copying CoStar content and populating X’s database.
The Very Next Day Xceligent’s Founder and CEO Was Fired

October 23, 2017

Xceligent Contractor Supports CoStar's Data Theft Claims

October 24, 2017

Doug Curry Out As Xceligent CEO

WILLIAMS & CONNOLLY LLP
After filing counterclaims against CoStar and vowing to fight back, Xceligent declared bankruptcy after its parent company wrote down its investment to zero.
Practice Pointers from the Xceligent Case

• Institute Protections With One Eye on Litigation
• Take Time to Build Your Record
• Evidence Can Be Seized and Preserved Before It Goes Missing
• Wrongdoers Can be Held Accountable—Across the Globe
Case Study 4: Database-Fraud Litigation

**Daily Dicta: Williams & Connolly Launches Litigation Blitzkrieg for CoStar (Pity the Defendants)**

CoStar files lawsuits from D.C. to California alleging widespread unauthorized use

**CoStar Starts Going After Password-Sharing Users In Latest Legal Blitz**
Seven Lawsuits, Across the Country, Filed on the Same Day

• First Wave:
  • Three cases in California, and one each in Oregon, New Jersey, Washington, DC, and Georgia

• Against individuals and companies, alleged to have:
  • Fraudulently accessed CoStar’s database
  • Downloaded thousands of pieces of data
  • Infringed CoStar’s copyrights

• Rejected CoStar’s reasonable efforts to end the theft without litigation
Legal Goals Checklist

- **Goal #1: Protect the IP.** Stop fraudulent access and prevent future misconduct.

- **Goal #2: Hold Fraudsters Accountable.** Recover from the individuals and entities that misused CoStar.

- **Goal #3: Educate the Market.** Demonstrate CoStar’s commitment to protecting its IP and illustrate the significant damages that come with accessing CoStar without proper credentials.

- **Goal #4: Develop Precedent.** Achieve results that can be used in future cases.
Developing the Evidence

• **IP Addresses.** Access to CoStar using subscriber credentials from an IP address affiliated with a non-subscriber

• **Device Affiliations.** Access to CoStar using subscriber credentials from a device (e.g., laptop, cellphone) affiliated with a non-subscriber

• **Device Names.** Subscriber registers a device with a name related to the non-subscriber

• **Other evidence.** Search histories, calls to CoStar
Developing the Evidence—Choi & Sandbox

Initial Findings

• Credentials of two CoStar subscribers used to access CoStar’s database from IP addresses and devices affiliated with a non-subscriber (Choi)

• Search histories of CoStar subscribers included a folder labeled with the initials of Choi

• Dueling logins: Access credentials would be used to attempt logins from different IP addresses in different geographic locations at the same time

Further Findings

• Review of records indicate that Choi created property reports containing CoStar-copyrighted photographs
Choi & Sandbox—A Chronology

• **Summer 2018**
  - CoStar detects unauthorized access and writes to Choi
  - No resolution, as Choi claims it is an “accident”

• **Summer-Fall 2018**
  - CoStar develops evidence of sustained unauthorized access and infringement

• **October 3, 2018**
  - CoStar files suit against Choi and his company, Sandbox Real Estate

• **November 13 & 16, 2018**
  - Choi and Sandbox served

• **January 4, 2019**
  - Stipulated judgment and permanent injunction entered; no discovery needed
"Defendants acknowledge that their actions constitute a serious violation of CoStar’s Terms of Use” and that Choi’s actions violate the Copyright Act, Computer Fraud and Abuse Act, the New Jersey Computer Related Offenses Act, and constitute fraud, and that Sandbox aided and abetted Choi’s statutory violations.”
2. **Choi** is hereby ordered to pay **CoStar** the sum of **$300,000**

3. **Sandbox** is hereby ordered to pay **CoStar** the sum of **$500,000**

2. **Defendants** shall be permanently restrained and enjoined from (a) accessing any **CoStar Database** without authorization from **CoStar**; (b) sharing any username, password,

3. **Defendants** shall be further permanently restrained and enjoined from infringing, by any means, directly or indirectly, any exclusive rights under the Copyright Act in any of **CoStar's copyrighted photographs**.

4. **If Defendants** violate either paragraph 2 or 3 of this Permanent Injunction, **Defendants** together shall pay **CoStar** the amount of **$50,000** (fifty thousand dollars) per infringing photograph per day of infringement, and **$50,000** (fifty thousand dollars) per real estate listing accessed, downloaded, or provided without authorization. This relief is non-
Practice Pointers from Database-Fraud Cases

- Develop and use a continuum of responses:
  - Technological defenses—IP blacklists and security modes
  - Confront apparent lone wolves and seek out-of-court resolution when the damage is not widespread
  - If a syndicate of bad actors, identify weaknesses in the group, but, if necessary, pursue simultaneously
  - Do not be afraid to litigate when appropriate

- Choose litigation candidates based on scope of misconduct and effect on company’s goals
- If litigating, develop complete record before suit
Conclusion

• Questions?
Jaye S. Campbell

Jaye is Deputy General Counsel and Head of Litigation for CoStar Group, an international provider of commercial real estate information, marketplaces, and analytics. Her primary responsibility is protecting, through legal and technological means, CoStar’s content, which includes a comprehensive subscription database of property photos and information and the content on dozens of websites in the U.S., Canada and Europe, including LoopNet.com, Apartments.com, and LandsofAmerica.com. She also has primary responsibility for disputes – big or small – involving CoStar, and leads antitrust matters, including interfacing with the FTC in pre-merger review and other contexts.

Originally from Texas, Jaye came to Washington, DC to attend college and never left. Her first client-service job was at Clyde’s in Georgetown, where she was a bartender.

Prior to joining CoStar, Jaye was an associate in the intellectual property group of Drinker Biddle & Reath LLP focusing on trademark and information technology matters.
Nick Boyle handles a wide variety of litigation, with an emphasis on complex civil cases with an international component. His experience spans federal and state courts around the United States; various arbitral fora—including AAA/ICDR, FINRA, JAMS, and ad hoc arbitrations; and, acting as coordinating counsel, courts around the world. In 2018 Nick was recognized by The National Law Journal as a “Trailblazer” for his pioneering legal strategy in global litigation over data theft by a client’s competitor. In 2016, Law360 featured Nick in its inaugural Trial Pros series, a Q&A highlighting his career as a trial attorney. Nick was also recognized as a D.C. “Super Lawyer” in 2017 and 2018. Nick co-chairs the firm’s Unfair Competition and Trade Secrets practice group.

Nick has represented investment banks, a global private equity fund, inter-dealer brokers, movie studios, technology companies, and the leading commercial real estate data provider. His practice encompasses commercial disputes; copyright and trade secrets cases, particularly involving the Internet; securities actions, including several RMBS cases; employment disputes in the financial sector; and defense of antitrust and RICO claims. His client representations take him to New York and London on a regular basis, and have also involved depositions and other work in multiple other locations from Australia to Estonia.
David Randall J. Riskin

An experienced commercial litigator at both the trial and appellate level, David Riskin manages complex matters in state and federal courts, with a particular focus on defending professional liability and conflict-of-interests claims against law firms. He engages all aspects of a matter by developing case themes, building expert strategies, preparing and defending key witnesses, and designing early-stage litigation strategies resulting in pre-trial dismissals and favorable settlements.

David’s broader commercial litigation experience has spanned a variety of industries, including financial services and securities, commercial real estate, medical devices, aerospace, healthcare, and technology. And he has represented individuals in civil, criminal, and governmental proceedings, both domestically and abroad.