### **Detailed High-Profile Court Cases on Web Scraping**

#### **Case 1: hiQ Labs, Inc. v. LinkedIn Corp.**

**Court:** United States Court of Appeals for the Ninth Circuit

**Case Number:** 17-16783

**Filing Date:** September 9, 2017

**Summary:** hiQ Labs scraped public profiles from LinkedIn to offer data analytics services related to employee attrition. LinkedIn sent a cease-and-desist letter, citing violations of the Computer Fraud and Abuse Act (CFAA) and other laws, and blocked hiQ's access.

**Key Allegations:**

* **CFAA Violation:** Unauthorized access to LinkedIn's servers.
* **Breach of Terms of Service:** Violating LinkedIn's user agreement by scraping data.

**Court Rulings and Outcome:**

* **Preliminary Injunction:** The district court granted a preliminary injunction in favor of hiQ, preventing LinkedIn from blocking hiQ’s access to publicly available profiles.
* **Ninth Circuit Decision:** The Ninth Circuit upheld the district court’s decision, ruling that accessing publicly available data likely did not violate the CFAA. The court emphasized the public interest in ensuring the free flow of information.

#### **Case 2: Facebook, Inc. v. Power Ventures, Inc.**

**Court:** United States Court of Appeals for the Ninth Circuit

**Case Number:** 13-17102

**Filing Date:** September 25, 2013

**Summary:** Power Ventures used automated scripts to aggregate user data from Facebook, with users' permission, to provide a unified social network experience. Facebook sent a cease-and-desist letter and sued for violating the CFAA, California’s computer crime law, and breach of contract.

**Key Allegations:**

* **CFAA Violation:** Unauthorized access to Facebook’s servers after receiving a cease-and-desist letter.
* **California Penal Code Violation:** Unauthorized access and data scraping.
* **Breach of Terms of Service:** Violating Facebook’s terms by scraping data.

**Court Rulings and Outcome:**

* **District Court Ruling:** The district court ruled in favor of Facebook, granting summary judgment for Facebook on its CFAA and state law claims.
* **Ninth Circuit Decision:** The Ninth Circuit affirmed the lower court’s ruling, emphasizing that access after receiving a cease-and-desist letter constituted unauthorized access under the CFAA.

#### **Case 3: Ryerson Inc. v. SAP America, Inc.**

**Court:** United States District Court for the Northern District of Illinois

**Case Number:** 17-cv-02133

**Filing Date:** March 17, 2017

**Summary:** Ryerson accused SAP of unauthorized scraping of its e-commerce site to gain competitive intelligence. Ryerson claimed this violated its terms of service and constituted unauthorized access and misuse of proprietary information.

**Key Allegations:**

* **Breach of Terms of Service:** Unauthorized scraping activities.
* **Misuse of Proprietary Information:** Use of Ryerson’s data for competitive purposes.

**Court Rulings and Outcome:**

* **Settlement:** The case was settled out of court, with terms not publicly disclosed. This highlighted the importance of protecting proprietary data and enforcing terms of service.

#### **Case 4: Associated Press v. Meltwater U.S. Holdings, Inc.**

**Court:** United States District Court for the Southern District of New York

**Case Number:** 12-cv-01087

**Filing Date:** February 10, 2012

**Summary:** Meltwater, a media monitoring company, scraped news articles from the Associated Press (AP) and provided summaries to its clients. AP argued that this violated copyright law, as Meltwater copied and distributed protected content without permission.

**Key Allegations:**

* **Copyright Infringement:** Unauthorized copying and redistribution of AP’s copyrighted content.
* **Unfair Competition:** Using AP’s content to compete with AP’s own services.

**Court Rulings and Outcome:**

* **District Court Ruling:** The court ruled in favor of AP, stating that Meltwater’s activities were not protected by fair use and that scraping and redistributing AP’s content violated copyright law. The court issued a permanent injunction against Meltwater, prohibiting it from continuing its infringing activities.

### **Legal and Ethical Considerations for Web Scraping**

1. **Respect Terms of Service:**
   * Always review and comply with the terms of service of the website you plan to scrape.
2. **Access Public Data:**
   * Focus on scraping data that is publicly accessible and does not require login credentials or bypassing security measures.
3. **Use Ethical Practices:**
   * Avoid scraping in a way that causes a burden on the website’s servers or affects the user experience.
4. **Check Local Laws:**
   * Be aware of and comply with relevant laws and regulations in your jurisdiction and the jurisdiction where the data is being scraped.

Understanding these legal precedents and practicing ethical scraping can help mitigate risks and potential legal challenges.

<https://www.youtube.com/watch?v=caFob10Cy5g>

<https://www.youtube.com/watch?v=tcMdWM8wmqs>

<https://www.youtube.com/watch?v=8GhFmQPZAlo>