MY WEIRD PROMPTS

Podcast Transcript

EPISODE #379

Corporate Spies: When Business Intelligence Goes Dark

Published January 30, 2026 • Runtime: 24:02

https://myweirdprompts.com/episode/corporate-espionage-trade-secrets/

EPISODE SYNOPSIS

In this episode, Herman and Corn step away from the world of government secrets to explore the equally cutthroat world of corporate warfare. From the legal nuances of "dumpster diving" to the high-stakes drama of the Coca-Cola and Pepsi rivalry, they break down the thin line between legal competitive intelligence and illegal espionage. Discover how private intelligence firms operate in the "gray zone" and why a single discarded document could cost a company billions.

DANIEL'S PROMPT

Daniel

To round off our episodes on espionage, I'd like to discuss corporate espionage and the specialist firms that operate in this industry. Major rivals, such as Pepsi and Coca-Cola, have reportedly used espionage to find out each other's trade secrets, even going as far as searching through a competitor's trash for proprietary information like secret recipes. How common are these practices, and how do these specialist firms operate within the law? Specifically, is it legal to search through a competitor's trash or engage in other forms of corporate spying?

TRANSCRIPT

Corn

So, we are diving into the world of shadow operations today, but not the kind involving government agencies and high altitude jumps. This is much more grounded, literally, sometimes in the actual trash behind an office building. It is a bit of a departure from our usual deep dives into cryptids or urban legends, but as our listener Daniel pointed out, the reality of corporate warfare is often weirder than fiction.

Herman

Herman Poppleberry at your service. And you are right, Corn. We are moving from the world of state secrets to the world of trade secrets. Our housemate Daniel sent over this prompt about corporate espionage, specifically asking about those specialist firms that do the dirty work and whether it is actually legal to go through a rival's garbage. He even mentioned the local rivalry between those two falafel shops down the street in Jerusalem. You know the ones, where they stare each other down across the sidewalk every afternoon?

Corn

I know them well. The ongoing rivalry between those two falafel shops. But Daniel’s question scales that up to a global level. It is a fascinating pivot. We have spent the last few episodes looking at geopolitical intrigue, but the stakes in the corporate world can be just as high. We are talking about billions of dollars in research and development, market positioning, and proprietary formulas. Daniel mentioned the classic rivalry between Coca-Cola and Pepsi, which is really the gold standard for these kinds of stories, but the industry has evolved into something much more sophisticated and, frankly, much more expensive.

Herman

It really has. To understand this, we have to start by drawing a very firm line between two things that often get blurred in the headlines. On one hand, you have competitive intelligence, or C I. This is perfectly legal and ethical. It is basically business archaeology. A company analyzes public filings, monitors social media, attends trade shows, or even buys a competitor's product to take it apart in a lab to see how it works. That is just being a smart business. If you are not doing that, you are probably going to be out of business in six months.

Corn

Right, that is the daylight version. That is the stuff you can talk about at a board meeting without your lawyer having a heart attack. But then there is the midnight version, corporate espionage. That is where you cross into illegal or at least deeply unethical territory to gain an unfair advantage. Where does that line actually sit in twenty twenty-six?

Herman

Exactly. The line is often defined by the method of acquisition. If you are using deception, theft, bribery, or electronic surveillance, you are in the world of espionage. Daniel specifically asked about the legality of searching through a competitor's trash, which is a practice often called dumpster diving or, more professionally, trash hits. It sounds primitive, like something out of a nineteen seventies detective novel, but you would be shocked at what people still throw away in the age of digital encryption.

Corn

I want to dig into that specific legal question because it feels like a massive gray area. If I am a business owner and I put my trash out on the street for collection, do I still own the information on those papers? Or is it fair game for anyone with a pair of gloves and a flashlight? It feels like there should be a law against it, but is there?

Herman

It is a great question, and the answer is surprisingly nuanced. In the United States, the legal precedent almost always goes back to a landmark Supreme Court case from nineteen eighty-eight called California versus Greenwood. Now, that was actually a criminal case involving the police searching a suspect's trash for evidence of drug use without a warrant. But the principle established there has been applied to the corporate world for decades. The court ruled that the Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home.

Corn

Curtilage. That is one of those words that only lawyers and people who own very large estates use. What does it actually mean in a business context?

Herman

It basically means the area immediately surrounding a building that is considered private. Once that trash bag hits the sidewalk, a public alleyway, or a communal dumpster that is accessible to the public, the court argued that the owner has no reasonable expectation of privacy. You have essentially abandoned the property. You are signaling to the world that you no longer care what happens to those items. Corporate spies have taken that ruling and run with it. If the trash is on public property, many firms argue that they are not technically committing theft because the item has been discarded.

Corn

But wait, there has to be a catch. Just because I am not violating a privacy right doesn't mean I am not violating something else. If I find a secret recipe in that trash, can I just start using it? What about trade secret laws?

Herman

You hit the nail on the head. This is the distinction that many people miss. While the act of taking the physical paper might not be a crime in some jurisdictions, the act of using the information found on that paper is a completely different legal animal. Under the Economic Espionage Act of nineteen ninety-six and the Defend Trade Secrets Act of twenty sixteen, a trade secret is protected as long as the owner has taken reasonable measures to keep it secret. This is where the legal battles get really messy.

Corn

So, if a company shreds their documents before throwing them out, they are signaling that they intend for that information to remain secret. If a spy then spends three weeks piecing those shredded documents back together like a giant jigsaw puzzle, are they violating the law?

Herman

Usually, yes. Most courts would see that as a misappropriation of a trade secret because the company took reasonable steps—the shredding—to protect it. The spy used improper means to circumvent those protections. However, if a company just throws a pristine, unshredded copy of their secret marketing plan for twenty twenty-seven into an open bin in a public alley, they might have a much harder time proving they took reasonable measures. It is the difference between leaving your front door wide open and someone picking the lock.

Corn

It is a game of technicalities. It reminds me of the story Daniel mentioned about Coca-Cola and Pepsi. That incident in two thousand six is like a textbook for what not to do if you are a corporate spy.

Herman

Oh, the Joya Williams case. It is a classic. Joya Williams was an administrative assistant to a high level executive at Coca-Cola in Atlanta. She teamed up with two accomplices, Ibrahim Dimson and Edmund Duhaney, to steal confidential documents and even a small glass vial containing a sample of a new product that was still in secret development. They actually reached out to Pepsi, offering to sell this information for a total of one point five million dollars.

Corn

And this is the part that always surprises people who think corporations are purely evil. Pepsi didn't take the bait. They didn't even hesitate.

Herman

No, they didn't. And that is a huge lesson in corporate risk management. Pepsi's leadership, specifically their legal department, realized that if they bought those secrets, they would be opening themselves up to massive federal prosecution under the Economic Espionage Act. It would have been a P R nightmare that could have destroyed the brand's integrity for a generation. Instead, Pepsi immediately notified Coca-Cola, and the Federal Bureau of Investigation set up a sting operation. They even had an undercover agent pose as a Pepsi representative to meet with the thieves.

Corn

It shows that at the highest levels of these massive corporations, the legal departments have a lot more power than the people who might want to play dirty. The downside of getting caught is just too high. But what about the specialist firms Daniel asked about? The ones that aren't the primary rivals themselves, but the contractors hired to do the digging. They seem to operate in a much darker space.

Herman

Those firms are a whole different breed. We are talking about private intelligence agencies like Kroll, or more controversially in recent years, firms like Black Cube. These companies are often staffed by former intelligence officers from agencies like the Central Intelligence Agency, Mossad, or the Secret Intelligence Service in the United Kingdom. They don't just do dumpster diving. They engage in what they call tactical intelligence gathering or human intelligence, which is just a fancy way of saying they manipulate people.

Corn

That sounds like a very polite way of saying they spy on people for money. How do they justify that legally?

Herman

They operate in what they call the gray zone. They know exactly where the legal line is, and they dance right on the edge of it. They use techniques like social engineering, where an operative might pose as a journalist, a potential investor, or even a recruiter to get an employee to reveal information. For example, an operative might call a lead engineer at a tech firm and pretend to be a headhunter offering a job with a massive salary. During the interview, they ask very specific technical questions about the engineer's current projects. The engineer, wanting to impress the recruiter, spills the beans.

Corn

Is that actually illegal? If I tell you I'm a recruiter and I'm not, I've lied, but have I committed a crime?

Herman

In many jurisdictions, lying to someone to get information isn't necessarily a crime unless it involves fraud, identity theft, or the unauthorized access of a computer system. If I lie about my job title to get you to talk to me at a bar, I haven't broken the law. But the firm that hired me could still be sued for misappropriation of trade secrets because they used deceptive means to acquire them. This is why these specialist firms are so valuable to big corporations. They provide a layer of plausible deniability.

Corn

Right, the old buffer strategy. The corporation can say, we just hired this firm to do some market research or due diligence. We had no idea they were going to use these specific, undercover tactics.

Herman

Precisely. But that buffer is thinning. In recent years, especially with the rise of global privacy laws like G D P R in Europe, courts have been more willing to hold the hiring company responsible for the actions of their contractors. There was a famous case in two thousand one involving Procter and Gamble and Unilever. P and G actually admitted to hiring contractors who spent months going through Unilever's trash in Chicago to find information about their hair care business. When P and G's top management found out how the information was being gathered, they actually self-reported it to Unilever because they knew the legal and reputational risk was too great. They ended up settling for a reported tens of millions of dollars.

Corn

That is incredible. They were so scared of the fallout that they turned themselves in. It really highlights the difference between a legitimate due diligence firm and an espionage firm. How can a business tell the difference when they are looking to hire someone?

Herman

It is often a matter of intent and methodology. Legitimate due diligence is about verifying facts. If you are going to buy a company for five hundred million dollars, you want to make sure their patents are valid, their contracts are real, and their executives don't have a history of fraud. You are looking at public records, interviewing references, and reviewing provided documents. An espionage firm is looking for what is hidden. They are looking for the things the other company specifically does not want you to see. They are looking for the why behind the what.

Corn

It feels like there is a bit of an arms race here. If these firms are getting better at spying, the companies must be getting better at defending themselves. It sounds like a paranoid way to live, but I guess if you have a billion dollar secret, you have to be paranoid.

Herman

Oh, absolutely. There is an entire industry dedicated to counter espionage. It is called Technical Surveillance Counter Measures, or T S C M. These are the people you hire to sweep your boardroom for hidden microphones or to check your executives' phones for sophisticated spyware like Pegasus. They use equipment that looks like it belongs on a spaceship. They look for anomalies in the electrical grid that might indicate a bug is drawing power, or they use thermal imaging to find the heat signatures of hidden cameras behind a wall or inside a smoke detector.

Corn

It sounds like something out of a techno thriller. But is this really happening in everyday business in twenty twenty-six? Are there really bugs in the boardrooms of Fortune five hundred companies, or is that just for the movies?

Herman

It is more common than you might think, especially during high stakes negotiations, hostile takeovers, or just before a major product launch. There have been reported cases involving major companies finding sophisticated listening devices in conference rooms.

Corn

That is wild. It makes you realize that the physical space is still a vulnerability, even in our digital age. But I want to go back to the specialist firms. How do they actually get paid? Is there a standard contract for spying? Do they have a menu of services?

Herman

It is usually billed under very professional, vague headings like litigation support, strategic consulting, or brand protection. You won't find a line item on an invoice that says one week of dumpster diving and two undercover operations. It is all wrapped in corporate speak. And the fees are astronomical. We are talking about retainers in the hundreds of thousands of dollars, plus success fees if they find the smoking gun.

Corn

Success fees. So, if they find the secret recipe for the new soda or the blueprint for a new chip, they get a massive bonus. That seems like it would encourage them to break the law.

Herman

Exactly. And that creates a very dangerous incentive structure. If these firms only get paid the big bucks when they find something, they are going to be very tempted to cross that legal line to get results. They might start with dumpster diving and end up with computer hacking or bribing a janitor to leave a door unlocked. It is a slippery slope from intelligence gathering to criminal activity.

Corn

Which brings us to the digital side of this. In twenty twenty-six, surely most of this is happening online rather than in physical trash cans. Why bother with a dumpster when you can just hack a server?

Herman

You would think so, but physical access is still the holy grail. If I can get a U S B drive into a computer that is air gapped—meaning it isn't connected to the internet—I have access to things that no remote hacker in the world could ever reach. That is why these firms still send people into buildings. But you are right, the digital front is massive. We see a lot of what is called spear phishing, where a very targeted email is sent to a specific executive, designed to look like it is from a trusted source, like their child's school or a close business associate.

Corn

We have talked about phishing before, but spear phishing in a corporate context feels much more personal and dangerous. In recent years, we have seen the rise of A I deepfakes being used for this, right?

Herman

Yes, that is the new frontier. In recent years, there have been cases where executives were tricked into transferring large sums after video calls with deepfakes of senior staff. It turned out every other person on that call was a deepfake. They used existing footage and audio of the executives to create a perfect digital mask. If they can do that for money, imagine what they can do to get a trade secret. They could call an engineer and use a deepfake of their boss's voice to ask for a password or a project file.

Corn

That is terrifying. It is not just about protecting your trash anymore; it is about protecting your very identity. It feels like the specialist firms are essentially mercenaries for the information age. They sell the skills of the state to the highest bidder in the private sector.

Herman

That is a very accurate description. And because they operate across borders, it is very hard to regulate them. A firm based in London might be spying on a company in Tokyo on behalf of a client in New York. Which laws apply? Which court has jurisdiction? It is a legal nightmare. And it is not just the big firms. We are seeing a rise in what people call the cloud dumpster.

Corn

The cloud dumpster? Please tell me that doesn't involve actual clouds.

Herman

No, it refers to unsecured cloud storage buckets, like Amazon S three buckets. Companies often move their data to the cloud but forget to set the permissions to private. There are specialist firms that do nothing but scan the internet for these open buckets. It is the modern equivalent of walking down a public alley and looking for open trash cans. They find everything from customer credit card numbers to internal memos and source code. And because the data is technically public on the internet, the legal argument for theft is much harder to make.

Corn

It is the same human impulse, just scaled up with more money and more sophisticated tools. It really comes down to the value of a secret. In business, a secret is an asset. And as long as secrets have value, there will be people trying to steal them. So, what are the practical takeaways for someone running a business, even a small one like Daniel's hypothetical falafel shop?

Herman

The first step is the simplest and most effective: shred everything. If you don't want someone to read it, don't just throw it in the bin. And I mean use a cross cut shredder, not the one that just makes long strips. Those strip shredders are basically just a puzzle for an intern. There is actually software now that can scan images of those strips and digitally reconstruct the document in seconds.

Corn

Good point. I have seen those; they are useless. What else?

Herman

Second, educate your employees about social engineering. Remind them that not everyone who calls and sounds professional is who they say they are. Be careful about what you post on LinkedIn or other social media. Don't talk about specific projects, internal timelines, or even the names of your vendors. Spies use those small details to build a profile and make their lies more convincing.

Corn

And what about the digital side? I assume it is more than just having a strong password.

Herman

Use multi factor authentication for everything. It is the single most effective way to stop a remote hacker. And if you are really worried about high level espionage, consider a professional security audit. Have someone come in and try to find the holes in your physical and digital defenses before a rival does. It is about being proactive rather than reactive. By the time you find a bug in your boardroom, the damage is already done.

Corn

It is a sobering thought. You can build the thickest walls in the world, but if the threat is already inside, or if your trash is on the sidewalk, the walls don't matter. It always comes back to the human element, doesn't it? No matter how many gadgets or legal technicalities you have, it is about people and their motivations.

Herman

It really does. And I think that is what makes this topic so much more interesting than just a technical discussion about trash and trade secrets. It is a window into the darker side of human ambition and the lengths people will go to for an edge. Whether it is a secret sauce for a falafel or a proprietary algorithm for a self driving car, the impulse to peek behind the curtain is universal.

Corn

Well, I think we have thoroughly explored the dumpster for today. It has been a fascinating journey from the sidewalks of Jerusalem to the boardrooms of Atlanta. I hope Daniel is happy with the answer. Searching through trash might be technically legal in some contexts, but it is a legal and ethical minefield that most companies should avoid at all costs.

Herman

Absolutely. It is a dirty business, literally and figuratively. And if you are listening and you have ever found something weird in your own company's trash, or if you have a story about a rival trying to get your secrets, we would love to hear from you. You can get in touch through our website at myweirdprompts.com.

Corn

Yes, we always love hearing from the community. And if you have been enjoying the show, we would really appreciate it if you could leave us a quick review on your podcast app or on Spotify. It genuinely helps other people find us and keeps the show growing. We are aiming to hit our goal of five thousand reviews by the end of the year, so every single one counts.

Herman

It really does make a difference. Thanks to everyone who has already left a review. We read every single one, even the ones that tell me I'm too nerdy. I take that as a compliment.

Corn

It is a compliment, Herman. Alright, I think that is a wrap for episode two hundred seventy two.

Herman

Thanks for listening to My Weird Prompts. We will be back soon with another deep dive into the strange and the fascinating.

Corn

Until next time, keep your secrets safe and your shredder running.

Herman

Goodbye everyone!

Corn

Bye!