MP SPY ACADEMY

Condition Yellow: What you see is data. What you understand is power.

THE READ

For the women who learned to read the room,

who saw what others missed,

who asked the hard questions,

and who refused to look away.

Five AM Clarity

The rain in Seattle in March is not dramatic. It does not crash or pound. It comes at five in the morning like a thought Maya Chen cannot shake, persistent and quiet, the kind that follows her through the dark streets of Wallingford at a pace somewhere between jogging and meditation.

Five AM was not an aesthetic choice. She had tried the evening gym, the weekend runs, the motivational apps with synthetic voices congratulating her on consistency. None of it stuck. Morning was different. Before the city woke, before the emails and calls and questions accumulated, before she had to be anything other than a woman moving through space at her own rhythm, her brain had room to work.

The route was the same most days: down Woodland Park Road, through the green belt where the city's edges got soft, back along the pond where the light came up slow and pink. This morning the pond reflected nothing. The sky was the color of old concrete. Rain fell in single droplets that seemed to come from nowhere, that seemed less like weather and more like the atmosphere had decided to weep without conviction.

She had learned to love running in Seattle rain rather than despite it. The rain here was not competition. It was context. Other runners saw weather as an obstacle to overcome, a test of their willpower. She saw the rain as permission to move at her own pace, to think while moving, to let her body work while her mind processed the accumulated disorders of her clients' data.

The route took her past houses where lights were starting to come on, past the sound of early-morning alarms and shower pipes and the first wave of people climbing out of sleep. Most of them would not leave for thirty minutes. Most of them would consume coffee and check their phones and read news that would make them anxious before they faced the day. She was already on the other side of that equation. By the time most people woke, she would have burned through the static in her head and had her best thinking done.

By the time she reached her building, her lungs burned in a way she recognized and appreciated. The burn meant the run had been hard enough to matter. Her legs had that feeling of useful fatigue, the kind that came from work rather than injury. She climbed the external stairs to her apartment on the third floor, moving quietly out of habit, though her neighbors were probably already awake. People who lived in the Wallingford area tended to be the type who woke early: professionals, parents, insomniacs masquerading as morning people. Successful people who had learned to optimize their sleep patterns. People who understood that the early hours belonged to whoever wanted them badly enough.

Euler was waiting at the door with the expression of a cat who had been gravely wronged by three hours of solitude. He was a Russian Blue, silver and elegant, and he performed disappointment with Shakespearean commitment. His eyes were accusations. His meow was the sound of profound betrayal. She had left him with a full bowl and fresh water. This was irrelevant to his sense of grievance. She fed him fresh food anyway, the small ritual that would allow them both to move forward, and showered quickly with water hot enough to open her lungs.

The apartment was still dark. The rain had turned the morning into something that felt like evening. She dressed in the clothes she had laid out the night before: dark jeans, a grey merino sweater from a company that promised

it would never stink, which had turned out to be true even after two years of frequent use, and her work boots with the worn soles that had traced through a thousand hours of Seattle sidewalks.

By six thirty, she was at her desk with coffee from the place two blocks down that made it correctly, meaning they did not try to improve it with art or foam or oat milk alternatives. The coffee was black and bitter and it worked. It was simple in the way that good work was simple: it did exactly what it was supposed to do without apologizing for its severity.

Her apartment was organized the way her mind worked: clean surfaces, everything with a purpose, nothing decorative. The living room held her couch, a side table, the cat tree Euler pretended not to use though she had occasionally discovered him on the top shelf at three in the morning, staring at her in the dark like some kind of furry sentinel. The kitchen was small and functional, just enough space to prepare food without feeling like you were cooking in a closet. The bedroom was bedroom-shaped, a place to sleep and nothing more. The home office where she spent most of her time contained her desk with its three monitors, her filing system organized by client and date, and a poster from her MPSA Analyst ribbon training she had attended three years ago. The poster showed a woman in silhouette with the text: "Condition Yellow: What you see is data. What you understand is power."

She had chosen the MPSA Analyst ribbon deliberately after leaving the bank. Most people would not have understood why. Most people would have looked at her career trajectory and seen a detour. But she had understood, even then, that reading data and reading people came from the same skill set, and that skill set could be applied in any direction depending on how much you wanted to push. The Analyst ribbon had taught her to push in the direction of answers rather than accusations. That was the only difference between an investigator and a conspiracy theorist: methodology, and the willingness to be wrong.

She opened her email. There were forty-three new messages since she had checked at nine PM the night before. This was not unusual. This was her life: people with problems, most of them related to data. Too much of it, too little of it, data in the wrong hands, data that should not exist in the first place. She read

through them quickly, sorting by urgency. A client had discovered that their payment processor was selling anonymized customer data to brokers; Maya had been with them through the contract negotiation and knew their options were limited. A law firm wanted her to analyze the metadata on a document set that would be used in litigation; this was routine work, the kind she could do in her sleep. A woman had emailed from a school district saying she had heard through a professional contact that Maya did work in data privacy and had a "unique analytical perspective."

The woman's name was Priscilla Holt. She was the superintendent of the Cascadia School District.

Maya slowed down on this one. She had learned to recognize the way certain emails carried weight that other emails did not. The weight was not in the words. It was in the spaces between the words, in what was written and what was left to be inferred. She read Priscilla's email carefully, once through to get the surface meaning, then again, slower, looking at the structure.

"I hope this message finds you well." Professional. Not warm, not cold, just precisely adequate.

"I heard about your work from a colleague who spoke highly of your analytical skills and your approach to data privacy issues." Someone had recommended her. Not a direct referral, which would have been more personal, but a recommendation that had traveled through enough intermediaries that it could be denied if necessary.

"We are currently undertaking a data audit related to a new educational technology contract." Current. New. Educational technology. The words chosen with care. Audit rather than investigation. Contract rather than problem.

"The district has the budget. They valued discretion. They were prepared to move quickly." This was the real paragraph. This was where Priscilla was saying: We have money. We can keep quiet. We need this done immediately.

The email was professional and carefully worded. It did not promise much and did not ask for much either. It asked if Maya would be available for a preliminary consultation on a data audit related to a new educational technology contract. Nothing in the email suggested that something was wrong.

Everything in the email's structure suggested that something was wrong.

Maya read it three times. She did this with emails, the way other people read contracts, looking for the sentence underneath the sentences. In this one, she found: We are concerned about something. We do not know what. We cannot talk about it through official channels. We need someone who can read what is hidden.

This was the kind of work she did best. Not because she was better at finding crimes, but because she understood that the absence of obvious problems was often the biggest problem. Companies failed, people went to prison, data got stolen, not because of spectacular errors, but because of careful architectures designed to hide ordinary decisions. Her job was to look at those architectures and understand what they meant.

She replied to Priscilla Holt's email with her availability and her rates. The rates were high, but they were honest. They reflected the reality of work that required her to think carefully about things and then to think about them again, and then to change her mind if the second thinking contradicted the first. She did not charge by the hour because that incentivized talking rather than thinking. She charged by the scope of work, which meant she had to understand the scope before she agreed to it. This usually meant being slightly more expensive than competitors and having the kind of clients who could afford to think long-term.

The rest of the morning unfolded as mornings did. She called the client with the payment processor problem and told him what he already suspected, which was that his contract allowed the broker arrangements and he would have to decide if he wanted to fight it or switch providers. Fighting would mean litigation. Switching would mean finding a new processor and migrating data. Both options were bad in different ways. She had learned that her job was not to solve problems but to help people understand what the actual choices were.

She reviewed a section of the litigation metadata, looking for inconsistencies in the document sets. She made more coffee, the second cup slower than the first, the kind of coffee you drank while thinking rather than while waking up.

By noon, she had heard back from Priscilla Holt. Would next Tuesday work? The district could provide access to all necessary files and systems. They were located in Shoreline. Dr. Holt would meet her personally to brief her on the scope.

Tuesday was four days away. Four days for Priscilla to be worried about whatever she was worried about, four days for the problem to exist in the space between discovery and action. Maya confirmed the appointment and added it to her calendar, which was still mostly empty, the way she preferred it. Her business came in waves: months of intense work followed by months of relative quiet that she used to take contracts that interested her rather than contracts that paid well, though ideally both qualities aligned. This wave was about to start. She could feel it.

She made lunch: a salad with careful portions of protein and vegetables, the kind of meal that made a statement about being a person who had her life organized. She ate it at her desk while reviewing her notes on the MPSA Analyst ribbon. She had completed it three years ago, right after leaving the bank. The decision to do so had seemed important at the time. Six weeks, intensive, taught by operatives and faculty who worked in actual intelligence and law enforcement and corporate security.

The Analyst ribbon had not been about technology. That had surprised her. She had expected it to be about tools and techniques. Instead, it had been about methodology. How to observe using the Ten-Second Scan and Corridor Protocol. How to construct timelines. How to find the patterns that made people's behavior intelligible. How to understand that people were almost always consistent, even when they were lying. The lie was usually consistent too. You just had to find what they were consistent with.

One of the instructors, a former FBI analyst named Sandra Voss, had pulled her aside on the last day of the training and said, "You see people clearly. That's unusual. That'll be useful if you can keep it from making you cynical."

Maya had nodded, accepting the compliment without saying that she had never been that innocent to begin with. She had worked fraud detection at a

bank. Four years of reading transactions, finding the signatures of dishonesty in the data. People were mostly consistent, and when they stopped being consistent in certain ways, it meant something. Fraudsters, for instance, usually had a moment where they shifted. One moment they were managing money normally. The next moment they started taking small amounts that they thought no one would notice. The small amounts meant they had crossed a line in their own minds. After that, the amounts got bigger, the timing got bolder. They were confident because they had already gotten away with something, and confidence made them less careful.

She had learned to read that transition in the data. She had learned that the data was not abstract. It was a record of decisions. Decisions meant intention. Follow the intention and you followed the crime.

By evening, Euler demanded dinner with increasing vocal intensity. He had learned that escalation was an effective strategy. A meow was insufficient. A series of meows, each more aggrieved than the last, would eventually produce results. Maya fed him again and made a reservation at a restaurant that served good Thai food and did not play aggressive ambient music or insist that you like their playlist. She texted her neighbor Tomás Reyes to see if he wanted to join her. Tomás was a contract attorney, rumpled and decent, the kind of man who would help you move even though he would complain about it the entire time, and who would remember important details about your life even when you did not expect him to remember them.

He said yes immediately, which meant he had nothing else going on, which meant he would be available if she needed him, which was why she had asked in the first place. Tomás was the kind of person who understood that "want to get dinner" sometimes meant "I'm thinking about something and could use someone to think about it with," and he was the kind of person who was fine with that arrangement.

They met at the restaurant at seven. Tomás was there already, reading something on his phone with the expression of someone reading something he did not like. He was wearing a jacket that had seen better days and pants that seemed to have been chosen for comfort rather than aesthetics. This was his default state. Tomás believed that clothes should function and that fashion was

a conspiracy designed to make you spend money on things that served no purpose.

He looked up when she sat down.

"You look like you're thinking about something," he said.

"I'm always thinking about something," Maya replied.

"This is different. This is your 'I'm going to do something interesting' face," he said. Tomás had known her long enough to have classified her expressions into categories. This was the kind of attention to detail that made him a good lawyer and a better neighbor. "Also, you're sitting like you're about to accept a job that's going to take up most of your time for the next several months."

"I'm sitting the way I always sit," she said.

"Exactly," he said.

She ordered pad thai and told him about the email from Cascadia School District. Tomás listened carefully, which was his professional skill and his most annoying personal habit. He did not interrupt. He did not offer unsolicited advice. He waited until she was finished and then he said, "They're covering something up."

"Presumably," Maya agreed. "Or they're worried about something they don't understand yet."

"Those are usually the same thing," he said. "Someone knows something is wrong, but they're not sure what it is or how wrong it is. That's when they call people like you."

They ate dinner and talked about the usual things: his work, her work, a case he was handling that involved a contract dispute with fascinating subtext about who had authority to make which decisions, a client she had fired six months ago for being unable to accept data that contradicted her preferred narrative. That was the hard part about the work. Most people wanted confirmation. They wanted you to look at the data and tell them they were right. When the data said something else, they either wanted you to reinterpret the data or they wanted to stop paying you. The ones who could handle the data when it was wrong were rare.

By the time they left, it was dark and the city had settled into the kind of quiet that meant it was a weeknight. The rain had stopped, leaving everything wet and reflective. The streets smelled like concrete and wet leaves.

"You'll tell me if it gets complicated?" Tomás asked as they walked back toward their building, their pace matching, neither one needing to look at the other to communicate pace.

"If it gets complicated, I'll need legal advice," Maya said. "Which means I'll be calling you anyway."

"I'm charging double for work you already know you're going to need," he said.

"Fair," she said.

She left him at his door and climbed the stairs to her apartment, where Euler had knocked her coffee mug off the desk in revenge for evening abandonment. She cleaned up the mess, the coffee having mostly dried into a stain on the hardwood, and sat down at her desk again. The apartment was quiet around her, the kind of quiet that belonged to the city at night. Outside, the March rain had started again, quiet and persistent, the kind that would continue until morning.

She opened a file labeled "Cascadia" where she would keep notes on the contract audit before she had even started. She created sections: Contract Review, Technical Assessment, Data Flows, Risk Analysis. She did not know yet what the contract would say or what she would find, but she knew how to look.

Outside, the March rain continued, persistent and quiet. Tomorrow she would run again, and the day after that, and the day after that. The pattern would hold until it didn't. She understood that about patterns. They were reliable until they broke. She had no idea yet that this contract audit would break everything else. But the rain seemed to know. The rain always seemed to know.

The Contract

The Cascadia School District occupied a modern building in Shoreline that had probably cost more than it should have and looked less impressive than it was intended to. The architecture was the kind that believed in open concepts and natural light, which translated to a lot of glass and a perpetual temperature of either too warm or too cold. There was no stable equilibrium. The building seemed designed to remind people that environmental control was impossible, that you could build whatever system you wanted but entropy would always win eventually. Maya preferred buildings that committed to their choices. This building was trying to be everything to everyone, which meant it was being nothing to anyone.

The morning was grey, typical Seattle April, the kind of weather that made you question whether the sun was a real thing or just something people remembered from childhood. Maya sat in her car for a moment before getting out, watching the building. The lobby had large windows. She could see people moving inside, the choreography of an institution starting its day. Administrators arriving early. Maintenance staff finishing their night shift. Secretaries settling in at their desks.

She arrived fifteen minutes early, which meant she had time to deploy the Ten-Second Scan in the lobby. The way staff moved told her about power structures. The tone of the voices in conversation told her about comfort levels. The physical arrangement of the front desk relative to the administrative hallway told her whether information flowed easily or was gatekept. These things mattered because they predicted behavior at scale. Institutions with tight information control usually had tight decision making. Institutions with open information flows usually made decisions by consensus, which was better for transparency but worse for speed.

This building leaned toward openness, which often meant insecurity hiding behind transparency. She had seen it before in her bank work: institutions that acted open because they had not yet understood they were doing something they needed to hide. The openness was a confidence strategy. If you act like you have nothing to hide, people assumed you were hiding nothing. But it was a strategy that broke down the moment the hiding was discovered. And Priscilla Holt, by hiring her to audit Axiom's contract, had suggested she believed hiding was occurring. The real question was not whether hiding was occurring. The question was what was being hidden and how deep the hiding went.

Priscilla Holt came down the hallway at exactly the appointment time, which told Maya something about precision and control. The punctuality was not accidental. Priscilla had planned to arrive at exactly the moment when the appointment began, which suggested someone who managed time the way she probably managed everything else: with intention and care.

Priscilla was 52 but had the polished appearance of someone who had long ago decided what version of herself she would present to the world and had been remarkably consistent about it. Her grey hair was styled in a way that looked effortless and professional, the kind of styling that required regular maintenance to stay effortless. Her jacket fit perfectly, tailored to her frame with the kind of precision that suggested a good tailor and the money to keep using them. Her shoes were expensive in the way that expensive shoes were subtle: you noticed the quality of the leather before you noticed the price. You did not notice that they had cost four hundred dollars until you thought about

shoes and realized that only expensive shoes felt that way on the feet.

She looked like someone who had a five-year plan and had executed the first two years successfully. Or the first three. Her bearing suggested someone who had accomplished what she had set out to accomplish and was now thinking about what came next.

Maya assessed her as she walked, reading the Biometric Leakage. Priscilla's shoulders were held carefully, not quite tense but not relaxed either. Her breathing was controlled, the kind of breathing you did when you were managing yourself. Her expression was pleasant but not warm. These were the micro-movements of someone who was managing her presentation very carefully. Maya had learned to read these involuntary signals through her Profiler ribbon training. Priscilla was worried about something. Priscilla was a person who did not usually allow worry to show in her face. The fact that Maya could see the worry suggested that the worry was substantial, that it had exceeded Priscilla's capacity to manage it completely, that something about the situation was making normal control difficult to maintain.

"Ms. Chen," Priscilla said, extending her hand. "Thank you for coming on short notice."

"I had availability," Maya said. They shook hands. Priscilla's grip was professional: firm but not aggressive, warm but not inviting. Not the grip of someone trying to prove something. Just someone who knew how to shake hands. "Your email was vague, which made me curious."

"I was being cautious," Priscilla said. "Would you like coffee before we start?"

They went to her office, which was corner position with a view of the parking lot and a door that closed. The positioning told Maya a lot. Corner offices meant power or at least the appearance of it. The door meant privacy was valued. The view of the parking lot rather than a city view or a view of the district meant she was focused on operations, on the machinery of the institution, not on aesthetics or status symbols.

Priscilla poured coffee from a carafe that looked genuinely fresh, not the coffee that had been sitting in the pot since dawn, that had developed a film and

tasted like burnt caramel. She handed a cup to Maya and sat across from her at a desk that was clean but not empty. The cleanliness meant organization. The non-emptiness meant current work, not just theater. Priscilla's desk held documents in folders, a calendar that was actually being used, a photo of what was probably her family, a single pen in a cup that held only that one pen. Everything was functional. Nothing was decorative. This was a woman who did not waste space or time on things that did not serve a purpose.

The coffee was still hot. Priscilla had made it not long before the appointment, which meant she had expected this meeting to matter, that she had taken the time to prepare properly. Maya added that to the constellation of small observations. Everything about Priscilla suggested someone who was careful and who prepared for important moments.

"I'm going to be honest with you," Priscilla said. "I don't know exactly what I'm concerned about. That's partly why I called you. I have instinct. I have a sense that something is wrong. But I need data to justify acting on that sense. If I go to the school board and say, 'I have a feeling,' I'll be dismissed. So I need you to help me either confirm that I'm being paranoid or confirm that my paranoia is justified."

"That's reasonable," Maya said. "Tell me what triggered the concern."

"We're contracting with a company called Axiom Learning Solutions," Priscilla began. "They provide adaptive learning software that personalizes student instruction. The school board approved the contract in the fall. It covers forty-one schools across our district, approximately thirty-eight thousand students from kindergarten through twelfth grade."

Maya was listening, but she was also watching, applying Kinesic Logic to read the body language. Priscilla's breathing was steady. Her hands did not move unnecessarily. She was uncomfortable but controlled. She was someone who had learned to compartmentalize worry. That was a useful skill in administration but it made it hard to read what you were actually worried about.

"The contract value?" Maya asked.

"Seven point two million over three years," Priscilla said. "It was the result of a competitive bid process. Three companies bid. Axiom was the most comprehensive solution and the most cost-effective. The board was enthusiastic."

Enthusiastic was interesting. Boards were usually not enthusiastic about things. Boards were cautious and consensus-driven. Enthusiasm suggested that someone had done good sales work. Or that the board was eager for something and that eagerness had made them less careful.

"But you weren't," Maya said.

"I wasn't," Priscilla confirmed. "Not because of anything specific. More because something felt off. And I have learned, in my career, that when something feels off, it usually is off. But I also understand that a superintendent cannot walk into a public board meeting and say, 'I have a feeling.' I need data. That's where you come in."

Maya made a note on her tablet: "Intuition triggered by what." She looked at Priscilla. "Tell me what felt off."

"Axiom's CEO," Priscilla said. "Garrett Sable. He was too smooth. Too enthusiastic. And he made a comment during the board presentation that stuck with me. He was talking about the learning algorithm and how much data it collects to personalize instruction. He said, 'The more we know about each student, the more we can serve their individual needs.' And then someone asked him about data privacy, and he said something like, 'We take student privacy very seriously. All data is anonymized and stored securely.' But the first comment was about knowing about students. The second comment was about anonymizing data. Those are not the same thing."

Maya understood immediately. Knowing was about information collection. Anonymizing was about information protection. The two statements were contradictory unless you understood that knowing was the goal and anonymizing was just the cover story. Priscilla was right. That was off.

Maya added to her note: "Contradiction between data collection purpose and privacy claims."

"Walk me through the contract," Maya said. "What data is being collected? Where is it stored? Who has access?"

Priscilla opened a folder on her desk and slid a thick document across to Maya. It was the kind of contract that had been written by lawyers who were paid by the word. The document had to have been over a hundred pages. The font was small. The paragraphs were nested like matryoshka dolls, each one containing subclauses that referenced other clauses.

"The official contract language says this," Priscilla said. She had highlighted key sections. "Axiom collects student learning data: assessment scores, time on task, wrong answers and patterns in wrong answers, navigation choices within the software, interaction duration and frequency. All of this is supposed to be used to generate personalized learning pathways."

Maya flipped through the document. The language was careful. It used the word "may" frequently, which meant it did not explicitly say what Axiom was collecting, but it did not exclude anything either. The contract was written in a way that preserved maximum flexibility for the contractor while appearing to constrain them.

"Storage location?" Maya asked.

"Their servers," Priscilla said. "Cloud-based, encrypted. They provide quarterly security audits from a third-party firm."

"Did you review the audits?"

"No," Priscilla said. "Which is part of why I called you. I don't have the technical expertise to evaluate a security audit. And it occurred to me that I should."

Maya made another note. She would want to see those audits. She would want to understand what they measured and what they ignored. Security audits could be theater. They could measure what they wanted to measure and overlook everything else.

"Who at Axiom would I contact to start the technical review?" Maya asked.

"Garrett Sable would route you to their Director of Data Operations," Priscilla said. She handed Maya a business card. "His name is James Porter. I

can email him to tell him you're coming, or you can contact him directly. Whatever makes sense."

"What did you tell anyone about why you're bringing in an outside auditor?" Maya asked.

"That we wanted an independent verification of our security posture," Priscilla said. "Which is true. But no one knows that I specifically am concerned. As far as the board knows, this is routine. As far as Axiom knows, this is standard district diligence."

"Good," Maya said. "Let's keep it that way."

She spent the next two hours with Priscilla, going through the contract and the implementation materials Axiom had provided. Axiom had provided extensive documentation: technical specifications, setup guides, privacy policies. The more she read, the more she understood Priscilla's intuition.

The data collection was extensive. Beyond the learning data, Axiom was also collecting demographic information, login patterns, and something the contract euphemistically called "contextual learning indicators." That phrase was vague enough to mean almost anything. Maya had learned to be suspicious of phrases like that. Usually they meant the company wanted to collect information but did not want to explain what information or why.

The access controls were not specified. The contract said "authorized personnel" could access data, but it did not say who "authorized personnel" were or what they could do with the data once they had it. It was a blank check with no constraints except that someone somewhere had deemed them authorized.

The data retention policy said data would be retained "for the duration of the contract and for archival purposes thereafter," which meant indefinitely. Archival purposes could mean anything. It probably meant never.

"When does the contract begin?" Maya asked.

"July first," Priscilla said. "In about three months. We're still in the setup phase."

"Good," Maya said. "That gives us time. I'll contact James Porter and tell him I need full technical documentation and access to do an independent

security audit."

"Will they give it to you?" Priscilla asked.

"They'll have to," Maya said. "If they don't, that tells us something too."

She stood to leave. Priscilla walked her to the door. The superintendent's office was on the tenth floor. The windows showed the parking lot and the street beyond, the everyday machinery of the district's operations. Somewhere below, forty-one schools were running their normal schedules, students were sitting in classrooms, learning data was about to be handed over to a company that was structuring itself in ways that made Priscilla Holt uncomfortable.

"If you find something," Priscilla said quietly, "you'll tell me before you tell anyone else."

"Yes," Maya said.

Driving back to Seattle, Maya ran through the contract in her head. She had done enough of these audits to recognize the signature of something being hidden. It was not in the things that were explicitly bad. Those would be obvious. It was in the gaps, the careful phrasings, the distinction between what the contract promised and what the contract allowed. It was in the carefully structured ambiguity that allowed someone to look at the contract and see what they wanted to see while the company looked at the contract and saw permission for something entirely different.

The drive back to Seattle took forty minutes. Maya used the time to think through what a complete audit would require. She would need to see the actual data schema, the fields being collected, the structure of the database. She would need to understand the security architecture, not just the claims about security but the actual implementation. She would need to trace where the data flowed, what happened to it as it moved through systems, who could access it, and what they could do with it once they had access. She would need to understand the corporate structure, who owned Axiom, what their incentives were, whether there were subsidiary companies or shell structures designed to hide things. She would need to understand who was involved in the decisions that had been made and what they had to gain from those decisions.

The Interstate 5 bridge stretched ahead of her, the city skyline appearing and disappearing in the grey afternoon. Somewhere in the audits she had done before, there were patterns she could apply here. The bank had taught her that fraud was not usually technical. It was usually structural. It was not someone figuring out how to steal money. It was someone building a structure where stealing money was easier than not stealing it. Once the structure was in place, the theft became inevitable. The question was just whether the theft would be small or large, quick or slow.

By the time she reached her apartment, she had a list of questions and the beginning of a plan. She would request technical documentation. She would ask for data samples. She would review the security audit. She would look at Axiom's corporate structure. She would find out who else was receiving data and why. She would build a timeline of decisions. She would trace money and incentives. She would look for the moment where the company had decided to become something other than what it claimed to be.

She opened her laptop and created a new file: "Cascadia: Axiom Learning Solutions Audit." She labeled the sections: Contract Analysis, Technical Review, Corporate Structure, Data Access Patterns, Risk Assessment, Timeline of Decision Making, Incentive Analysis.

The sections were mostly empty. But she knew how to fill them. It would take time. It would require patience and careful observation. It would require the kind of thinking that the MPSA Analyst ribbon had taught her: the assumption that people acted in their interests, and the question was always what their interests actually were. This was the foundation of the Operative Mindset Triad -- Clarity about motive leading to Control of her investigation and the Choice of what to investigate next. Garrett Sable was acting in his interests. James Porter was acting in his interests. The venture firms funding Axiom were acting in their interests. The question was not whether they were acting in their interests. The question was what their actual interests were and how those interests had shaped the decisions that were being made.

Euler demanded dinner with his usual insistence. She fed him and made coffee and then sat down at her desk. Outside her window, the city was moving through evening. Street lamps came on. The rain continued. The darkness

deepened.

She made coffee and settled in to work. Outside, the March rain continued into April. Inside, Maya Chen began to read a contract very carefully for all the things it was trying not to say. She understood that the contract was a narrative. Someone had written it with a purpose. The question was what that purpose was. What story was the contract trying to tell? And what story was it trying to hide?

James Porter

Axiom Learning Solutions occupied the ninth and tenth floors of a building near Safeco Field, in that particular Seattle neighborhood where tech companies had moved once the downtown core became too expensive and too congested. The building was glass and steel and new enough to look like it had been purchased yesterday. There was probably a plaque somewhere with the architect's name and the year of construction and some statement about innovation and design excellence. Maya had always thought that tech companies chose their real estate the way they chose everything else: to communicate wealth and competence and the knowledge that they were correct about the future.

The building was designed around the principle that success looked like transparency. All the interior walls were glass. All the meetings were visible. Everyone could see everyone else working. The open plan was meant to break down silos and encourage collaboration. It was meant to communicate that there was nothing to hide. Maya had learned that the desire to communicate that you had nothing to hide was usually inversely correlated with actually having nothing to hide. The most transparent-seeming spaces often concealed

the most. The surveillance panopticon disguised as openness.

She had emailed James Porter three days after meeting Priscilla Holt. The email had been carefully written to communicate authority without aggression: she was an independent auditor hired by the district, she needed to review the technical security and data handling implementation, she would be discreet. The discreet part was important. It suggested that she understood the business world understood these audits as routine and that she would not make a big deal out of things. It suggested that she was not here to find problems but to verify that they did not exist.

James had replied within an hour: he would be happy to facilitate the audit. He had suggested this week. He had offered to bring in Axiom's CTO, Daniel Kim, to answer technical questions. The quick response was interesting. The eagerness to cooperate. The offer to bring in the technical expertise. These were not the responses of someone who was trying to hide things. Or they were the responses of someone who believed the things they were hiding were hidden well enough that scrutiny could not uncover them.

This was good. This was the response of a company that believed it was doing nothing wrong. Or the response of a company that believed it could handle scrutiny because the wrong they were doing was hidden well enough. Either way, it was a response that suggested she would get access to what she needed. Access was the point. If she could see how the system worked, she could understand what it was doing.

James Porter was waiting in the lobby when Maya arrived. He was a man in his early forties, wearing the tech industry uniform: expensive jeans that had been worn in a way that looked natural, a button-up shirt with the sleeves rolled, sneakers that cost more than they looked like they did. He was clean in a way that suggested a personal trainer and a good gym membership. He had the appearance of someone who had been told he was good at his job and had decided to believe it. His smile was the smile of someone who had practiced his social skills in exactly the right amount of detail to make them seem natural.

"Ms. Chen," he said, standing to greet her. "Welcome to Axiom. We're excited to facilitate your audit."

"I appreciate the access," Maya said. They shook hands. His grip was the grip of a man who had been taught the importance of handshakes, the precise amount of pressure that communicated confidence without aggression. "I'll try not to be too disruptive."

"No disruption at all," James said. "We're proud of our security practices. The more transparency, the better."

He took her up to the ninth floor and gave her the tour. The office was open concept: desks arranged in clusters, no one behind closed doors, glass conference rooms with names like "Learning" and "Growth" and "The Synapse." The naming was interesting. The Synapse. That was a reference to how neurons connected. It suggested that the office itself was meant to be a network of connected ideas. It was the kind of naming that told you what the company wanted to believe about itself.

He pointed out the different teams: Product, Engineering, Data Science, Operations. She watched the employees as James walked her through. Most of them looked young, early career, the kind of people who had probably come to Axiom because it was well-funded and seemed like it had interesting problems. They were working at their desks, in conversations, collaborating on whiteboards. They looked engaged. They did not look like people who suspected they were part of something wrong.

"We're about 150 people," James said. "We've grown quickly, but we try to maintain the culture that got us here."

"Which is?" Maya asked.

"Education-first thinking," James said. "We believe that data can unlock each student's potential. Everything we do is oriented toward that goal."

That was the stated mission. Maya made a mental note: stated mission versus actual business model would be worth examining. She had learned at the bank that the gap between stated mission and actual practice was where the interesting things lived.

She followed James to a conference room on the tenth floor. Daniel Kim was already there, setting up his laptop and a collection of whiteboards and diagrams. Daniel was older, maybe late forties, with the unhurried demeanor of

someone who had solved technical problems for decades and knew most problems could eventually be solved if you were patient enough. He had the kind of bearing that came from experience. He was not trying to impress anyone. He just understood that his knowledge was valuable and did not need to perform that value.

"So," Daniel said, "you want to understand how we're storing student data."

"That's the starting point," Maya said. She opened her laptop and started taking notes. She would need the technical specifications, but more importantly she would need to understand the decisions that had been made. Every technical decision was a choice. Every choice reflected priorities. If she understood the priorities, she understood what the system was actually designed to do.

For the next eight hours, Daniel walked her through Axiom's technical architecture. The depth of his explanation suggested that he was either very proud of the work or very thorough. Possibly both. Most engineers who were thorough about their work also took pride in it. That was how you got thoroughness, by caring enough about the quality to actually do the work properly.

The data came in from the district's student information system through an encrypted API. It was stored in a cloud database, encrypted at rest and in transit. The encryption used current standards: AES-256 for storage, TLS 1.3 for transmission. These were good choices, the kind of encryption that would actually protect data against external attackers. The keys were managed by a hardware security module. That was also a good choice, a device that made it harder to steal the encryption keys. Access was controlled through role-based permissions, a standard approach where different users had different access levels based on their role in the company. There were audit logs that tracked every access, a record of who accessed what data and when. There were quarterly penetration tests conducted by a third-party firm, external security testing to look for vulnerabilities. There were backup procedures and disaster recovery plans in case the primary system failed.

It was all properly built. It was secure against external threats, against hackers trying to break in from the internet, against competitors trying to steal the data. It was security designed to keep the data safe from outside intrusion.

It was, technically speaking, well-built. The kind of infrastructure that would cost significant money to implement correctly. The kind of infrastructure that required real expertise to maintain. And that was the problem.

As Daniel explained the system, Maya asked questions that seemed procedural but were actually architectural. How many people had access to the master keys? What logs were kept for administrative actions? Were the logs themselves protected? Who could modify the audit logs? What about the backup data, where was it stored, who could access it?

Daniel answered each question carefully, and with each answer, Maya could see the system that was being described. It was not a system designed to protect student privacy. It was a system designed to allow data access while leaving a record that appeared secure. There was a difference, and the difference was everything. A privacy-focused system would have been designed to make data access difficult. This system was designed to make data access easy while recording that access had occurred.

"How much student data are you storing?" Maya asked.

"Assessment data, learning engagement data, timestamp information," Daniel said. "Everything needed to drive the adaptive learning algorithm."

"Roughly how many fields per student?" Maya asked.

Daniel consulted with James. James said, "I'd have to check our latest schema. Probably two hundred fields? It varies by grade level."

Two hundred fields. That was not assessment data. That was a comprehensive profile. Assessment data would be fifty fields, maybe seventy-five. Two hundred fields meant you were collecting information about behavior, psychology, family situation, everything about the student that could possibly be measured or inferred.

"Can I see the schema?" Maya asked.

"That's proprietary," James said immediately. The response came too fast, which meant James had already thought about whether the schema could be shared and had decided it could not. "But we can give you a de-identified sample of the data structure."

"I'll need to see the actual schema to properly assess risk," Maya said. "And I'll need it marked as confidential if that's a concern. But you can't audit data security without understanding what data you're securing."

James and Daniel exchanged a look. The kind of look that meant they were checking with each other without speaking. Daniel was uncomfortable. James was deciding what to do.

"Let me talk to Garrett," James said. "I think we can work something out."

"Who is Garrett?" Maya asked, though she knew.

"Garrett Sable. Our CEO. He'd want to approve sharing that level of detail," James said.

"Of course," Maya said. She made a note of the resistance. Proprietary information was a shield, and shields usually meant something worth protecting. She had learned this at the bank: when someone would not show you something, they were usually trying to hide something. It did not mean they were doing something illegal. It meant they were doing something they did not want you to see. "In the meantime, can I see the third-party security audit?"

"I'll have that sent over today," Daniel said.

They broke for lunch. James ordered Thai food and they ate in the conference room. The conversation drifted toward Axiom's mission and market position. Axiom had been founded six years ago by Garrett Sable and a technical co-founder who had since moved on. The move-on was interesting. Usually it meant conflict or that the technical person had made their money and decided to move to something else. James did not elaborate and Maya did not ask.

The company had grown through a combination of legitimate product innovation and well-executed sales work. School districts were the early market. Axiom was now positioning itself to expand into corporate training,

university learning outcomes assessment, and workforce development.

"We have investors," James said, "who see the potential of this technology across industries. Once you've built a behavioral model for a student, the same model can apply to understanding employee engagement, customer preferences, anything where human behavior is the variable you're trying to optimize."

"So the learning algorithm is portable," Maya said.

"Exactly," James said. He seemed genuinely pleased by her understanding. "The algorithm is agnostic to context. You train it on student behavior. You can deploy it on employee behavior. The underlying math doesn't change."

That was the real business model. The algorithm was not about learning. It was about behavioral modeling. The learning was just the training ground. Once you had an algorithm trained on student behavior, you could apply it anywhere humans had behavior that could be measured.

"And your investors are?" Maya asked.

"Mix of venture firms and strategic partners," James said. "Garrett would have the full cap table."

Maya made another note. She would want to see the cap table. She would want to know who owned Axiom and what they expected to get out of a behavioral modeling system deployed across 38,000 children. Strategic partners was a phrase that could mean anything. It could mean other companies that wanted to use the algorithm. It could mean companies that wanted to buy the data. It could mean something entirely different.

She spent the rest of the afternoon collecting documents: contract terms, technical specifications, security audit reports, privacy policy. By six o'clock, she had filled three folders and gotten a good sense of the Axiom operation. It was competent. It was well-funded. It was building something that looked like an educational tool but functioned as a comprehensive behavioral profiling system. The pieces did not fit together unless you understood that fitting together differently than the public story suggested.

Daniel walked her to the elevator. He had been quiet during the lunch conversation, less engaged than he had been during the morning technical explanation. During lunch, when James had been talking about the applications for behavioral modeling, Daniel had been looking at his phone, his attention elsewhere. That absence of attention was itself data. Daniel Kim did not want to hear about the future of what Axiom was building. Daniel Kim had already decided he did not like that future.

"I know this seems paranoid," he said quietly, "but data security is not paranoia. It's caution."

"I appreciate that," Maya said. "And I appreciate the honesty."

"There's something you should know," Daniel said. He was looking at the elevator doors, not at her. The avoided eye contact was interesting. It suggested that what he was about to say carried weight for him, that he had made a decision to tell her something that he had decided not to tell others. "When I started here, we were building a learning tool. A good one. The algorithms were designed to help students learn more effectively, to personalize instruction, to identify gaps in understanding. It was the kind of work that felt like it mattered. I was working on something that I believed in.

"But somewhere along the way, the focus shifted. Somewhere between the Series A and the Series B funding, the entire company had a pivot moment where the focus moved from learning to data. Now I build infrastructure that does things I'm not entirely sure about. I stay because I have a family and because telling myself that the data is anonymized is easier than looking closely at what we're actually doing with it. I stay because leaving would mean admitting that I work for a company that I'm uncomfortable with. And I'm not strong enough to do that."

The elevator doors opened.

"If you find something," Daniel said, "take it seriously. Don't assume we have safeguards we don't actually have. Don't assume that the people who built the system intended for it to be used in the way the company is using it. And don't assume that having people who are uncomfortable with what's happening means the company is going to change."

"I'll be thorough," Maya said.

She rode down to the lobby and drove back across the bridge to Seattle. The afternoon traffic was heavy. The car moved in slow waves, stopping and starting, the rhythm of rush hour in the city. She had time to think about everything she had seen.

What she was thinking was that Daniel Kim had just told her the thing that mattered: somewhere along the way, Axiom had stopped being a company focused on education and started being a company focused on something else. She did not yet know what that something was, but she knew now that it existed. Daniel had confirmed it through his discomfort, through his need to explain why he was staying at a company where he was building infrastructure for something he was uncomfortable with. That was not the response of someone who was confident the company was doing nothing wrong. That was the response of someone who had compromised with themselves so many times that compromise had become the default position.

She got home, fed Euler who expressed his displeasure at her late arrival with a pointed ignoring of her presence, and opened her laptop. She created a new section in her notes: "Behavioral Profiling." Under it, she wrote: "Two hundred fields per student. Agnostic algorithm. Portable across contexts. Investors interested in applications beyond education. Daniel Kim uncomfortable with direction of company. Suggests pivot happened between Series A and Series B funding."

Then she did something she had learned to do at the bank: she began to look for companies that might be buying what Axiom was selling. She started with the corporate structure. Axiom Learning Solutions was the public entity. But was there a subsidiary? A shell company? A separate holding company for data products? She opened her browser and started searching. It was eight o'clock in the evening. Euler had settled on the couch. The rain was falling on the windows. She had nowhere to be and all the time she needed to understand what Axiom was actually doing.

The Analyst

Two weeks into the audit, Maya had collected approximately four gigabytes of documents, schemas, access logs, and security reports. She had a timeline of when Axiom's business model appeared to shift, somewhere between their Series A funding and their Series B. She had identified three shell companies that seemed to be subsidiary entities but that did not appear in Axiom's official corporate disclosure.

What she did not yet have was specific evidence that Axiom was doing anything illegal.

This was a problem because Priscilla Holt would eventually ask for a conclusion, and Maya's conclusion so far was: "The company is structured in a way that allows data to be repurposed in ways the contract does not explicitly address, the technical security is sound but the governance is minimal, and something about the business model does not align with the stated educational mission."

That was intuition masquerading as analysis. She needed specifics. She needed evidence. She needed something that moved from suspicion to fact.

She was reviewing the schema for the hundredth time, looking for patterns in the data fields, when she got an email from a Gmail address she did not recognize. The subject line was: "Cascadia Audit."

She opened it carefully. Anonymous emails were a risk. They could be traps. They could be someone trying to manipulate her into confirming their existing beliefs. They could be someone's attempt to get her to leak information. But they could also be what they claimed to be.

"I heard you're auditing Axiom," the email began. "I work there. I can't send this from my work email. I don't want to be identified. But there's a lot you should know."

Maya's first instinct was to delete it. But she read the rest anyway, scrolling through carefully.

"I'm a junior analyst on the Data Operations team," the email continued. "I was assigned to the project to prepare the Cascadia district data for Axiom's use. While I was doing that, I discovered something that made me uncomfortable. I don't know if it's illegal, but it's definitely not what the school district agreed to.

"There are secondary processing systems that are not mentioned in the contract. The student learning data goes into the main database, which is what you've probably seen. But there's a separate pipeline that takes portions of that data and processes it through different algorithms. These algorithms are generating scores. The scores are for things like risk assessment, influence susceptibility, emotional state, family income proxy. The output is being fed to something called Project Cornerstone.

"I don't know what Project Cornerstone is. I only know that it exists and that the data from Cascadia is being fed into it. If you want to know more, I can try to get you samples, but I'd need to be careful. I don't want to lose my job, but I also don't want to be part of something that I'm not comfortable with.

"My name is Delia Park. I'm attaching a secure email address. If you want to talk, that's where you should reach me."

Maya read the email three times. Then she read it again, looking for the hidden tells. The writing was professional but not stiff. The person was clearly

educated. The person was clearly technically competent. The person was clearly scared. The fear came through in the specific details: mentioning the job loss risk, mentioning the discomfort, mentioning the uncertainty about whether it was illegal. All of that was the genuine emotion of someone who was taking a real risk.

This was the moment where she could close the file and call Priscilla Holt and say that she had found irregularities that suggested data governance could be improved. It was the moment where she could walk away, take her payment, move on to the next contract. The work would be satisfactory. The findings would be legitimate. The district would have a report that justified bringing in an outside auditor.

Instead, she forwarded the email to an encrypted mail service, created a new account with a secure provider, and sent Delia Park a message at the address she had provided.

"I'm interested in talking. What would make you comfortable?"

Delia's response came within an hour. "Coffee. Public place. Tomorrow morning."

They met at a coffee shop in the Beacon Hill neighborhood, neutral territory far enough from both Axiom and the school district that it was unlikely they would run into colleagues. The neighborhood was residential, the kind of Seattle place where people lived actual lives rather than performing their professional identities.

Delia was younger than Maya had expected, maybe 29, wearing jeans and a hoodie that made her look even younger, made her look like someone who had stumbled into corporate employment and had not yet decided if she was staying. She was holding a coffee cup in both hands like it was a comfort object. She had not slept much. The exhaustion was visible in her face, in the way her eyes were slightly unfocused.

"I'm scared," Delia said, not as a greeting but as the first true statement. "I don't want to be here, but I also don't feel like I can not be here."

"That's normal," Maya said. "Tell me what you saw."

Delia told her about the Project Cornerstone pipeline. She was technical enough to understand the data flow but not technical enough to fully understand what the algorithms were doing. She just knew that the school district data was being processed in ways that were not documented in the contract, that the output was being labeled with phrases like "risk assessment," and that the data was being fed somewhere she did not have access to.

The way she described it suggested she had observed the system without fully understanding its purpose. She had seen data going in. She had seen processing happening. She had seen outputs being generated and sent somewhere. But she had not been able to trace the entire path or understand the destination.

"Can you get me samples?" Maya asked.

"Maybe," Delia said. "It's risky. The system logs access. If I pull data, there's a record. But I might be able to do it in a way that looks like normal work. I'll have to be careful."

"How careful?" Maya asked.

"Very," Delia said. "If they catch me, they'll fire me. And they might do other things too. The company has lawyers. The company has resources. I don't."

Maya understood what Delia was really saying. The company had power. Delia had a job and a career and the normal vulnerabilities of someone who had spent the last few years building professional credentials. If Axiom decided to make an example of her, they could. They had the lawyers. They had the resources.

"If you get caught," Maya said, "you hire Tomás Reyes. He's a contract attorney. He's good. I'll make sure he knows to expect you."

"That assumes I know what I'm doing is actually wrong," Delia said.

"Is it?" Maya asked.

"I don't know," Delia said. "But it's secret, and secret usually means wrong."

That was the honest answer. Not a legal conclusion. Just the instinct of someone who understood that things worth hiding were usually worth hiding for reasons that would not hold up to scrutiny.

They did not exchange contact information. Instead, Delia said she would reach out through the encrypted email if she had something. She left first. Maya waited ten minutes and left after her, taking a different route home to ensure they were not followed, which was possibly paranoid but was the kind of paranoia that was sometimes justified.

That evening, Maya called Tomás and told him to expect that someone might contact him about representation related to a whistleblower situation. She did not tell him who or when, but she told him the person would mention her name and that he should take them seriously.

"You're assuming something is going to blow up," Tomás said.

"I'm not assuming anything," Maya said. "I'm preparing for probability."

Over the next week, Delia sent her encrypted messages with snippets of information. The data being fed into Project Cornerstone included the student demographic information, academic performance data, behavioral indicators, family income proxies derived from address and school lunch eligibility, emotional state assessments based on writing samples and classroom interaction patterns. All of it was being processed to generate scores.

The algorithms generated scores for "risk indicators," "influence susceptibility," "emotional stability," and something called "lifetime engagement potential."

Lifetime engagement potential. That phrase stuck with Maya. What did it mean to be engaged with something for a lifetime? What was the something? Was it a product? Was it a political candidate? Was it a brand? Or was it something more fundamental: a way of understanding how to keep someone engaged, how to understand what would make them responsive to messaging, how to create the conditions for behavioral influence across their entire lifespan?

"Can you get me documentation on what Project Cornerstone is?" Maya asked in one message.

"I'm trying," Delia responded. "But I don't have access to the high-level project documentation. I can see data going in and systems processing it, but not the strategy docs that would explain why."

"Look at file creation dates," Maya suggested. "Look at who created the secondary processing pipeline. Look at the internal communication about why it's separate from the main system."

Over the next two weeks, a picture began to emerge. Project Cornerstone had been created eight months ago, shortly after Axiom's Series B funding. The funding had come from a venture firm that specialized in AI and behavioral applications. The pipeline had been built by a subset of the engineering team, separate from the main product team. The secondary processing system was intentionally isolated from the main Axiom architecture.

Isolation meant security. It also meant secrets. It meant that the system was important enough to warrant special protection, but that protection went both directions. It protected the system from external threats, but it also protected the system from internal scrutiny. If only a small team knew about it, then only a small team could question it.

Delia managed to send her copies of the data schema for the secondary processing system. It was extensive. The fields included demographic breakdowns, academic performance patterns, behavioral markers, family economic status, address information that could be mapped to neighborhood demographic data, and then the algorithm outputs: risk scores, influence susceptibility ratings, emotional stability assessments.

Maya imported the schema into her own database and began to analyze what the system would actually do. If you fed that data through a behavioral model, what would you be able to predict? What would you be able to influence?

She built the model in her head first. Start with demographics. You knew where the student lived, which told you about their neighborhood, their socioeconomic status, their family structure based on proxy indicators. Add academic performance, which told you about their intelligence, their effort, their response to different types of instruction. Add behavioral indicators,

which told you about their self-control, their risk tolerance, their susceptibility to peer influence. Add emotional state assessments, which told you about their psychological vulnerabilities, their triggers, their likely responses to stress.

Then run that through an algorithm designed to predict influence susceptibility. What you would get was a comprehensive profile of every student's psychological vulnerabilities and behavioral patterns.

The answer was: everything. You would be able to predict vulnerability and target it. You would be able to understand which students were susceptible to persuasion. You would be able to understand family economics and target messaging accordingly. You would be able to build a complete profile of each student's behavior, psychology, and social position.

It was, in technical terms, a comprehensive behavioral modeling system. In practical terms, it was a system designed to understand and manipulate the population it was studying. It was the architecture for influence at scale.

Maya sat at her desk late into the evening, going through the data. She was thinking about Garrett Sable and his smooth presentation, about the careful language in the contract, about the isolation of the secondary pipeline. She was thinking about what an algorithm trained on this data could be used for. She was thinking about the answer to every question that mattered: who benefits?

She made a call to an old colleague at the bank, someone who had worked in the fraud detection unit and had since moved to the corporate security department at Amazon. She asked a specific question: if you were trying to build a database of psychological profiles and behavioral vulnerabilities on a population, what data would you collect?

Her colleague laughed. "We call that behavioral targeting. It's what every ad tech company does. Why do you ask?"

"Theoretical question," Maya said.

"The data you'd want," her colleague said, "is the same data that predicts fraud, except you're using it for influence instead of risk. You want demographics, financial indicators, educational history, behavioral patterns, emotional state if you can measure it, decision-making history. You want to know what triggers people, what they respond to, where their vulnerabilities

are."

"And if you had that data on thirty-eight thousand people, all of them under eighteen?"

There was a long pause.

"That would be valuable to someone," her colleague said carefully. "And concerning to everyone else."

Maya ended the call. She pulled up her analysis of Axiom's corporate structure. She looked at the three shell companies. She looked at the venture firm that had funded the Series B. She looked at the data about Project Cornerstone.

Then she wrote an email to Priscilla Holt. The subject line was: "Preliminary Findings. Need to schedule urgent meeting."

She attached a document labeled "CONFIDENTIAL ATTORNEY-CLIENT WORK PRODUCT" even though Priscilla was not her attorney. It was a protective measure. It would make it harder for anyone else to demand the document later. It would signal that this was sensitive. It would make it clear that she understood the seriousness of what she was about to say.

In the document, she wrote: "The contract audit has revealed significant discrepancies between the stated purpose of the Axiom Learning Solutions data collection and the actual system design. Secondary processing pipelines are extracting student data and running behavioral profiling algorithms that are not mentioned in the contract. The output appears to be psychological and demographic profiles that are being fed into a system called Project Cornerstone. I cannot yet confirm the purpose of Project Cornerstone, but the data being processed suggests it is designed for behavioral targeting and persuasion applications. I recommend the district immediately request an independent investigation into Project Cornerstone and I recommend the district consider suspending the Axiom contract pending resolution of these issues."

She sent the email at ten PM on a Thursday. Priscilla responded at six AM on Friday: "Can you come in Monday? I need to show this to the board legal counsel. I may also need to involve the superintendent of instruction. How

confident are you in this assessment?"

Maya responded: "Very confident in the architecture. Less confident in the purpose, but the architecture suggests the purpose is not educational. I have sources but they cannot be exposed without risk. More analysis would be helpful."

Priscilla's response came back immediately: "Keep analyzing. Say nothing to anyone except Tomás Reyes if you need legal advice. I'll be careful about how I present this. Thank you for taking this seriously."

That Monday, Maya met with Priscilla and two other people: James Chen, the superintendent of instruction, and Karen Park, the board's legal counsel. Karen was careful and precise and had the appearance of someone who had spent decades dealing with institutional liability. She had the bearing of someone who had seen institutions make bad decisions and who understood exactly what happened when they did. She asked good questions.

"Do we have evidence that data was actually transferred out of Axiom's systems?" Karen asked.

"Not yet," Maya said. "But the system architecture supports it."

"So you're working from design analysis, not evidence of actual transfer," Karen said.

"Yes," Maya said. "I can trace the data in, I can see the processing happening, I can see outputs being generated. I cannot see where the outputs go. But the system isolation suggests the outputs go somewhere intentional."

"That's weaker," Karen said. "They'll argue that the pipeline is for internal analytics and not for data export. They'll argue that no actual harm has occurred. They'll argue that their security prevents unauthorized access."

"The security prevents external unauthorized access," Maya said. "It does nothing to prevent authorized access by people who own the company."

"True," Karen said. "But that's not necessarily a contract violation if the contract allows data use for adaptive learning purposes and if they argue that behavioral profiling is necessary for adaptive learning."

"It is a contract violation," Maya said, "because the contract does not explicitly authorize behavioral profiling. It authorizes educational assessment data collection. What they're building is something different."

Karen nodded slowly. "You need stronger evidence. You need either actual documentation that Project Cornerstone is designed for non-educational purposes, or you need evidence that data is actually being transferred to external parties."

"I'm working on it," Maya said.

She left the meeting and went home and sat at her desk. The apartment was quiet except for the sound of rain on the windows. Euler had decided to forgive her for being gone most of the day and had settled on the back of her desk chair, close enough to be in the same space but not so close as to admit actual affection.

She looked at the data Delia had sent her. She looked at the corporate structure of Axiom. She looked at the venture firm funding the Series B. She looked at the business model that was emerging from the combination of all that information.

The venture firm was called Stratton Capital. They had a reputation for investing in companies that operated at the intersection of data and behavior. They had funded ad-tech companies. They had funded companies building recommendation algorithms. They had funded companies that built tools for understanding and predicting human behavior. If Stratton Capital had funded Axiom, then Axiom's pivot toward data was not an accident. It was aligned with what they wanted to see happen.

She pulled their recent SEC filings. She looked at their investor presentations. She looked at their other portfolio companies.

Then she started to follow the money. Money was never complicated. Money always made sense. Money always went toward the person or organization that could benefit most from having it. If you understood who had the money and what they wanted from it, you understood what was really happening in the deal.

The process would be slow. It would require patience. But the outline was becoming visible. What had started as an educational software company had been identified by venture investors as a potential behavioral data source. The company had been funded with that understanding. The company had then pivoted to monetize that data source. The data was being sold to organizations that wanted to understand and influence behavior. The students in the Cascadia School District were the raw material. Their behavioral data was the product.

It was an elegant system. It was evil, but it was elegant. And her job was to make the elegance visible, to show how each piece connected to every other piece, to demonstrate that this was not an accident or a misunderstanding but a deliberate construction.

The Thread

Delia managed to extract the information from the Project Cornerstone database without triggering immediate alarms, using a combination of careful query timing and disguising the data pull as routine system maintenance. The extraction was done late on a Thursday evening when most people had left the office, when the system logs would be less carefully reviewed, when the queries would be buried in the noise of actual maintenance operations. She was good at this kind of work. She had learned how systems kept secrets. She knew how to move through them without leaving visible traces.

She used a secure channel to send Maya a list of organizations that had received data feeds from the system. The list was attached as a spreadsheet, each entry marked with a date and a data volume, the recipient organization, and sometimes a brief note about what the data was being used for. The detail was remarkable. It suggested Delia had been careful. It suggested Delia understood what Maya would need to see.

The list was six pages long. Thirty-seven organizations total. Thirty-seven places where the behavioral data on thirty-eight thousand children had been

sent.

Maya read through it methodically, highlighting connections as she saw them. Political consulting firms: three of them, all mid-sized, all with clients running for office or advocacy campaigns. Microtargeting platforms: companies that specialized in voter targeting and consumer targeting, the kind of companies that worked for political campaigns and social media companies. Data analytics companies: firms that worked with commercial clients to understand behavior, to predict purchase patterns, to understand influence susceptibility.

And three organizations that looked legitimate on the surface but that did not appear to have clear business purposes. They were registered corporations, but there was nothing public about them. No websites. No LinkedIn pages. No obvious business model. No employees listed anywhere. Just shell structures that existed on paper and nothing more. But they were receiving substantial data volumes, hundreds of gigabytes, the kind of volume that suggested they were active operations, not just registered but dormant entities.

One name appeared twice: CrossStile Analytics.

CrossStile had received data from Project Cornerstone in March and again in June. The volumes were substantial. Hundreds of gigabytes in each shipment. That was not sample data. That was operational data. That was the kind of volume that suggested the data was being used to train or operate actual systems.

Maya ran CrossStile through her searches. The company was registered in Delaware as an LLC. The registered agent was a law firm that specialized in privacy and corporate law. There was no public website. There was no LinkedIn company page. There was no listing in business directories. It was a company that had been incorporated but had made no effort to have a public presence.

But CrossStile had received data from Project Cornerstone. And CrossStile was connected to something called Cornerstone Data Management, which was registered under different ownership but shared an office address in Arlington, Virginia. Arlington was where serious data companies lived. It was

where the infrastructure that powered political and commercial microtargeting was built.

And Cornerstone Data Management was connected to something called American Insights LLC, which was a data consulting firm that worked primarily with political campaigns and advocacy organizations. American Insights had a website. It had case studies. It had a clear business model: understand voter behavior, help campaigns understand their electorate, help campaigns target messaging to specific populations.

The network was there. She just had to trace it carefully enough that she could show it to people and they would understand what they were looking at.

She called Tomás at his office.

"I need to understand the corporate structure of data shell companies," she said. "Specifically, I need to know how to prove who actually owns them when the ownership is obfuscated."

"Why?" Tomás asked.

"Work," Maya said.

"Cascadia," Tomás said. It was not a question.

"Yes."

"Okay," Tomás said. "Come by my office tonight. I'll walk you through how to read Delaware corporate filings and how to cross-reference ownership through registered agents. It's boring but effective."

She met Tomás at his office in the Fremont neighborhood, in a building that had probably been converted from industrial use sometime in the last decade. The building had exposed brick and high ceilings and the kind of character that came from having a previous life. His office was small and cluttered, with files everywhere and an actual paper calendar on the wall. Tomás believed in maintaining records in ways that were difficult to digitize, which Maya had always suspected was more about habit than principle. Habit was often better than principle. Habit kept working even when principles wavered.

He spent two hours showing her how to trace corporate ownership through layers of indirection. Delaware made it easy for companies to hide behind registered agents. But the filings still had to list managing members, officers, registered agents. The filings had to be consistent across time, even as companies tried to obscure that consistency.

"The key," Tomás said, "is that they can change the names, but they usually keep the same registered agent. And the registered agent is a real person who actually exists and has other clients and other responsibilities. Once you identify the registered agent, you can follow them. They're usually the consistent thread."

He showed her examples. Companies that had multiple identities, multiple filings, multiple shell structures, all connected by the same law firm serving as registered agent. It was like following water. You could not create water, but you could follow where it flowed. You could trace it from the source to the destination even if the water itself kept changing form.

Maya went through the Axiom shell companies with this new knowledge. She found the registered agents. She found that the same law firm appeared across multiple companies. She found that the same lawyer appeared as the responsible party for both Cornerstone Data Management and CrossStile Analytics.

The lawyer's name was Martin Kessler. He was a partner at Kessler and Associates in Arlington, Virginia. According to his LinkedIn profile, he specialized in tech law and had worked for several venture-backed startups in the behavioral technology space. His job was to build the corporate structures that allowed information to flow while hiding who was actually benefiting from that information.

Maya sent Martin Kessler an email asking if he could discuss his work with Cornerstone Data Management in his capacity as a legal representative. She received an automatic response saying he was out of the office and would be back the following week.

She made a spreadsheet of the connections: Axiom to Project Cornerstone to CrossStile Analytics to Cornerstone Data Management to American Insights

LLC. She made a timeline of when each connection had been established. She made a column for "Known Purpose" and filled it in with what she could infer: American Insights worked with political campaigns. Cornerstone Data Management had data management contracts with political organizations. CrossStile Analytics served as a middleman distributing data.

The business model became clear once she organized it that way. Axiom collected behavioral and demographic data on students. Project Cornerstone processed that data through algorithms that generated behavioral profiles. CrossStile distributed the profiles to organizations that wanted them. Those organizations primarily appeared to be political campaigns and advocacy groups.

They were building detailed psychological profiles of 38,000 children and selling them to people who wanted to know how to influence those children's families. The students themselves were not the target. The families were the target. The data on the students was the mechanism for understanding and influencing the families.

It was worse than she had thought it was. Which meant it was probably a federal crime.

She called Priscilla Holt.

"I need to present what I've found so far," she said. "But I need to do it in a way that's secure. I need to understand what the district's obligations are regarding reporting this to law enforcement."

"Come in tomorrow," Priscilla said. "We'll bring in Karen Park. We also need to contact the superintendent and the school board president."

"The fewer people who know about this before I can present everything, the better," Maya said.

"I understand," Priscilla said. "But you're not the only one who's going to need to take responsibility for this."

That afternoon, Maya received an encrypted message from Delia Park.

"They know something is wrong. I overheard a conversation between James Porter and Daniel Kim. James is worried that someone pulled data yesterday. He was asking Daniel if there could have been an access that wasn't

recorded. Daniel said no, the logs are clean. But James was still worried. I think they're starting to suspect there's a breach."

That was the risk with whistleblowing. You could not take data without leaving traces. You could not hide the fact that you were the person who took it. The security systems that protected the data also exposed who accessed the data. Delia had bought time by disguising her access as routine work, but that cover would only last so long.

"How long do we have?" Maya asked.

"Hours maybe. Days at most," Delia said. "If they audit the access logs more carefully, they'll figure out it was me."

"Okay," Maya said. "Here's what you're going to do. You're going to call Tomás Reyes. You're going to tell him you need representation. You're going to tell him you may be involved in a whistleblower situation. You're going to stop accessing any Axiom systems immediately. And you're going to document everything you know about what you accessed and when you accessed it."

"And then what?" Delia asked.

"And then," Maya said, "we make sure that what you found gets used correctly."

She met with Priscilla, Karen Park, and James Chen on Thursday morning. She brought hard copies of all her analysis, printed out and organized in folders. She had learned from her MPSA Analyst ribbon training that sometimes the best way to present damaging information was in a way that forced people to sit with it, to look at each piece individually, to understand that this was not speculation or intuition but careful analysis backed by documents. This was the methodology of laying out evidence in a chain that could not be disputed.

They sat around Priscilla's conference table. Karen had her legal pads ready. James Chen had the expression of someone who was about to find out that something he had trusted was broken.

"Here is the corporate structure," Maya said, showing them the diagram she had created. "Axiom Learning Solutions is the operating company. But there are three shell subsidiaries. And those subsidiaries connect to a network

of companies in Arlington, Virginia."

"Here is the timeline of when Project Cornerstone was created relative to Axiom's Series B funding." She showed them the months, the dates, the way the project had been created within weeks of the new funding coming in. "Here is the list of organizations receiving data from Project Cornerstone. Here is evidence that these organizations include political consulting firms and microtargeting platforms."

She watched their faces as they absorbed it. Karen was leaning forward, reading carefully. James Chen was pale. Priscilla was composed but her breathing had changed.

"Here," Maya said, "is the data schema for the behavioral profiling system. Here is evidence of the data that's being extracted from the Cascadia district and fed into that system. Two hundred data fields per student. Not assessment data. Behavioral profile data."

"Is there a contract violation?" Karen Park asked.

"Significant ones," Maya said. "The contract explicitly authorizes data collection for adaptive learning purposes. What you're seeing here is data collection and processing for behavioral targeting purposes. The contract does not authorize that. The contract does not even acknowledge that that's a possibility."

"Is there anything illegal?" James Chen asked.

"I'm not a lawyer," Maya said. "But I believe the federal government would have significant interest in this. You're talking about detailed behavioral profiling of children. You're talking about data being sold to third parties without consent. You're talking about a system designed to understand how to influence people's behavior."

"What do you recommend?" Priscilla asked.

"Immediately suspend the Axiom contract," Maya said. "Secure all Cascadia student data in Axiom's possession. Notify the federal authorities. And protect the people who are providing you information, because they're taking significant personal risk to help you understand what's happening."

Karen nodded slowly. "We'll need to present this to the full board. We'll need to get counsel from outside firms. We'll need to move carefully because once we start this process, Axiom will have lawyers here immediately."

"I understand," Maya said. "But the data on thirty-eight thousand children is already in their system. Every day you wait is another day they have access to it."

They decided to move forward with a special board meeting on Monday. Priscilla would present the audit findings in closed session. Karen would advise on next steps. They would present the decision to suspend the contract to the full board on Tuesday in public session, which would force transparency and prevent Axiom from claiming they had not been given opportunity to respond.

Maya left the meeting and drove back to Seattle. She had done the analysis. She had found the evidence. Now she had to wait and see if the institution would actually do something with what she had found. She had learned that institutions often knew they were broken but found it easier to continue operating broken than to fix themselves. The repair required too much disruption. The admission of wrongdoing was too costly. It was easier to pretend things were fine and hope the problems did not become visible.

That evening, Euler knocked a glass of water off her desk and forced her to take a break. She fed him and made dinner and tried to sit with the fact that she had just set a process in motion that would be very difficult to reverse. Once you told the board, the board had to tell authorities or admit to knowing about a crime and covering it up. Once you told authorities, the authorities had to investigate. Once you investigated, things became public.

Her phone buzzed. A message from Delia Park: "I called the attorney. I'm scared but I'm also relieved. Is this normal?"

"Yes," Maya replied. "You did the right thing."

"How can you be sure?" Delia asked.

"I can't be sure of anything," Maya said. "But I'm sure that hiding it would have been the wrong thing. And I'm sure that you wanted to do the right thing. Sometimes that's enough."

She did not sleep much that night. She kept thinking about the architecture of what Axiom had built. She kept thinking about how it had probably seemed reasonable at each step, how each decision had probably felt like a small thing at the time. Expand data collection a little. Add a processing pipeline to serve adaptive learning. Monetize the algorithm because it was valuable. Sell to organizations who want to understand behavioral patterns. But somewhere along the way, small decisions had added up to something different: a system that could profile and influence people's behavior at scale.

That was how things usually happened. Not through one big decision, but through a series of smaller ones that each seemed acceptable until you stepped back and saw what you had built. Each person involved could tell themselves they were just doing their job, just building a technology, just creating business value. Daniel Kim could tell himself that he was just doing his job, just building secure infrastructure. James Porter could tell himself that he was just doing business development, just making the company successful. Garrett Sable could tell himself that he was just pivoting the business model to something more profitable, something more aligned with what investors wanted.

But when you put all those individual decisions together, they became a sentence that read: we are building a system to understand and manipulate people. And thirty-eight thousand children had been enrolled in that system without knowing it. Their data had been collected and processed and sold without the knowledge or consent of their families. The system had been built carefully, intentionally, with full knowledge of what it was doing and why.

The worst part was that it was all legal. Or at least, it would be difficult to prove that it was illegal. The contract allowed data collection. The contract allowed data processing. The contract was silent on data selling, which meant it did not authorize it, but it also meant Axiom could argue that the contract did not prohibit it either. The company had been careful. They had built structures that would make it difficult to prove crime even when the wrong was obvious.

That was why she did the work she did. Not because it was always clear what the law said. But because when the wrong was obvious enough, the law usually caught up.

The Board

The special board meeting was held in a conference room in the administrative building on Monday at six AM before the regular district business started. Priscilla had called it at the last minute, which meant it would not leak ahead of time. The full board was present: six members plus the board president, all of them looking confused about why they had been pulled out of bed early.

Robert Martinez was the board president, a man in his sixties who had spent a career in business before moving into public service. Susan Reeves worked in corporate law. David Wong was an engineer. There were three other members whose backgrounds were less obvious but who all had the look of people who took their volunteer positions seriously.

Maya was present as the consultant, but only after Karen Park had signed her to a temporary consulting retainer that made her attorney-client privileged. It was a technical move but an important one. It meant that if Axiom tried to discover her analysis, there would be legal barriers to it. It meant that her sources could be protected. It meant that the work was privileged communication and not subject to casual disclosure.

Priscilla presented the findings methodically. She explained the contract, the stated purpose of data collection, the technical discovery of secondary processing systems. She showed the data schema. She showed the timeline. She showed the organizational connections.

She walked through it slowly, giving the board time to understand each piece. This was not a presentation designed to move quickly. This was a presentation designed to force understanding. Each document was a piece of evidence. Each piece of evidence was part of a pattern. The pattern, taken as a whole, told a story that could not be misunderstood.

The board members' expressions changed as they understood what they were being told. This was not a minor compliance issue. This was not a vendor who had overreached or made technical choices that were questionable. This was a contract violation and possibly a crime.

"How confident are you in this analysis?" asked Robert Martinez, the board president.

"Completely confident," Maya said. She had learned when to sound certain and when to sound cautious. This moment required certainty. "I've reviewed the technical architecture. I've reviewed the corporate structure. I've reviewed the data being processed. This is not a misinterpretation. The secondary system exists. The data is being processed. The output is being sold to third parties."

"What are the implications?" asked Susan Reeves, a board member who worked in corporate law.

"Potentially significant," Karen Park said. "You're talking about the collection and sale of behavioral data on minors without parental consent. You're talking about data being used in ways that were not disclosed in the contract. You're talking about systems designed for psychological profiling and behavioral influence. Federal agencies would have substantial interest in this."

"What do we do?" Robert asked.

"First," Karen said, "we immediately suspend the Axiom contract. We send formal notice that we are suspending implementation pending review of contract compliance. We secure all Cascadia student data that's in Axiom's

possession. We notify law enforcement."

"Which law enforcement?" Susan asked.

"FBI," Maya said. "This is federal jurisdiction. It involves minors. It involves interstate commerce in data. It involves psychological profiling systems designed for influence. You're looking at potential violations of multiple federal statutes."

"And it will be very public," Robert said.

"Yes," Karen said. "Once you notify the FBI, it will eventually become public. You cannot keep something this significant quiet."

"Can we negotiate with Axiom?" asked David Wong, another board member. "Can we ask them to delete the data?"

"You can try," Karen said. "But I would not recommend it. You have a right to know the data has been misused. You have an obligation to your students' parents. You have an obligation to law enforcement to report potential crimes. Negotiating with Axiom before you've notified authorities puts you in a position where Axiom can claim they're cooperating in exchange for immunity."

The board sat with that for a moment. The implications were heavy. They were about to accuse a vendor of federal crimes. They were about to involve the FBI. They were about to make something that had been hidden become very visible.

But they were also a school board. Their responsibility was to students. Thirty-eight thousand students had been enrolled in a system that was processing their data in ways they did not know about. The parents of those students had given permission for educational data collection, not for behavioral profiling. The violation was clear. The response was clear.

The board voted unanimously to suspend the contract. They voted unanimously to notify the FBI. They voted to authorize Karen to immediately send formal notice to Axiom and to instruct Axiom to cease all processing of Cascadia student data.

The notice was sent at seven AM. By eight AM, Maya's phone was ringing. It was James Porter from Axiom.

"What the hell did you tell them?" he asked.

"The truth," Maya said.

"You don't know the truth," James said. "You don't understand what we're doing."

"Then explain it to me," Maya said. "Explain to me what Project Cornerstone is. Explain to me why you're building behavioral profiles on children. Explain to me why you're selling that data to political organizations."

There was silence.

"We're not selling the data," James said finally. "We're providing analysis services."

"That's a semantic distinction," Maya said. "You're taking data on students, processing it to create behavioral profiles, and providing those profiles to organizations that want to influence behavior."

"It's the same thing that Google does with ad targeting," James said. "It's the same thing that Facebook does."

"Yes," Maya said. "And there are significant legal and ethical questions about those companies too. But those companies aren't marketing to school districts as educational software while secretly building behavioral targeting systems. That's the difference."

"Garrett made a decision," James said. His voice had changed. He was less defensive now. He was resigned. "He decided that the educational software was not going to be profitable fast enough. He decided that the real value was in the data. I disagreed with that decision, but once it was made, I was already compromised. I couldn't blow the whistle without destroying my own future."

"I know," Maya said. "That's what always happens."

"What happens now?" James asked.

"The FBI investigates," Maya said. "Axiom cooperates. And Garrett Sable has a choice about whether to fight or to negotiate."

"I'm going to need a lawyer," James said.

"Yes," Maya said. "You're going to need a very good one."

By Tuesday morning, the story was already leaking to the local news. The Seattle Times had picked it up. The tech blogs were running with it. The school board was preparing for a public meeting where they would announce the contract suspension. Axiom was in crisis management mode, issuing a statement about how they took student privacy seriously and were committed to working with the district to resolve any concerns.

The statement was carefully worded. It did not deny anything. It just repositioned what had been done as something that they took seriously, which was technically true even if the seriousness had been insufficient. Axiom had taken privacy seriously. They just had decided that the value of the data was more important than privacy protection.

The FBI field office in Seattle had been notified and had opened an investigation. Agent Marcus Webb had been assigned to coordinate the response. He called Maya on Tuesday afternoon.

"I understand you're the consultant who discovered the irregularities," he said.

"Yes," Maya said.

"I need to see everything you have," he said.

"You'll need to work through the district," Maya said. "It's their data. But they've authorized me to cooperate with federal investigations."

"I'm coming to you first," Agent Webb said. "I want to see your analysis before I talk to the district. I want to understand your methodology. I want to know if there are gaps."

They met at a coffee shop in Capitol Hill on Wednesday morning. Agent Webb was thorough and careful. He was not one of the agents who assumed a civilian consultant was either incompetent or unreliable. He was the type who understood that good information could come from anywhere and that his job was to evaluate it carefully, not to dismiss it based on source.

He asked good questions. He understood the technical architecture quickly. He understood what the data meant. He understood the implications.

"This is solid work," he said when he was finished reviewing everything. "You found the hidden system. You traced the corporate structure. You

connected it to the recipients. This is what would have taken us weeks to construct on our own."

"I had a source inside Axiom," Maya said. "That's how I found the secondary pipeline."

"I'll need to interview that source," Webb said.

"The source is protected," Maya said. "They're already taking significant career risk."

"I understand," Webb said. "But they'll need to provide a statement at some point. Right now, I just need to know if there are any other systems I should be looking for."

"There could be," Maya said. "I found what I found by accident. If the system is well-designed, there could be additional processes I haven't discovered."

"Okay," Webb said. He made notes. "Here's how we'll proceed. We're going to execute a search warrant at Axiom's offices. We're going to secure their servers. We're going to interview staff. We're going to trace the money to understand who's been paying for this and what they've been using the data for."

"What about the data that's already been distributed?" Maya asked.

"That's the hard part," Webb said. "Once data is in the wild, you can't necessarily get it back. But we can identify where it went. We can identify who has it. We can determine if there are federal crimes involved."

The search warrant was executed on Thursday morning. The news coverage was immediate and extensive. "FBI Raids Ed-Tech Company Over Student Data Misuse." "School District Discovers Hidden Profiling System." "Axiom Learning Solutions Under Federal Investigation."

The public board meeting that night was packed. Parents came, angry and afraid. How long had their children's data been processed? What profiles had been created? Who had access to them? What would happen to the data? The questions came fast, layered with fear and anger.

Priscilla addressed the meeting with care. She explained that the district had discovered what appeared to be a contract violation. She explained that they had suspended the contract immediately. She explained that the FBI was investigating. She explained that the district was working to secure all student data and to understand the full scope of what had been processed.

She did not panic them. She did not minimize the problem. She just told them what had happened and what the district was doing about it.

She did not name Maya directly. But she did acknowledge that the irregularities had been discovered through an independent audit, and that the consultant who conducted the audit had acted with professionalism and integrity.

After the meeting, Priscilla pulled Maya aside.

"Thank you," she said. "You were right. And you moved fast enough that we were able to act before this got worse."

"The worst part," Maya said, "is that this was preventable. If the contract had been more carefully drafted. If someone had asked harder questions when Axiom's technical architecture didn't match the stated educational purpose. If anyone had been looking carefully at the way the data was being collected and used."

"That's always true," Priscilla said. "But that doesn't change what we do now."

Over the next week, more details emerged in the news and in the FBI investigation. The FBI had found evidence that Axiom had been selling behavioral profiles to political consulting firms for use in voter targeting. The evidence was in contracts. It was in data transfer logs. It was in communications between Axiom executives and the political firms, discussions of what data was available and how much it would cost to acquire it.

They had found evidence that Axiom had been working with a data broker to distribute student profiles to commercial interests. The broker was a company that specialized in acquiring data from multiple sources and bundling it into data packages that commercial companies could buy. If Axiom had student behavioral data and the broker could distribute it to corporations

interested in understanding consumer behavior, then the entire supply chain made sense. The students were the product. Their data was the product. The behavioral profiles were the product.

They had found evidence that Garrett Sable had made a conscious decision to pivot the business model from educational software to data brokerage. The decision had been documented. There were emails between Garrett and the venture investors discussing the shift. There were board presentations showing the financial projections for selling data versus selling educational software. The software model had limited upside. The data model had unlimited upside. Once you had the data, you could sell it repeatedly, to multiple customers, indefinitely. The data business was infinitely more profitable.

There was a moment where Garrett had stood in front of the engineering team and said: "The real value is not in the learning software. The real value is in the behavioral data. The learning software is the vehicle. The data is the product. We're not selling education. We're selling insight into how to influence students and their families."

Garrett had hired expensive lawyers. Axiom had suspended operations on Project Cornerstone pending the investigation's outcome. But the damage was done. The company's reputation was destroyed. Parents across the country were demanding to know if their districts were using Axiom. School boards were quietly auditing their contracts, checking what data they had given to Axiom, what assurances they had received. The venture firm that had funded the Series B was facing questions about how thoroughly they had understood what they were funding. They had understood perfectly, it turned out. They had understood that Axiom was pivoting to a profitable data business and had funded it accordingly.

Axiom Learning Solutions would not survive this. The company would fold or be acquired and restructured. The name would be ruined. The business would be over. Garrett Sable would face federal charges. Some of the engineers would face charges. Some of the executives would negotiate cooperation agreements with the federal government in exchange for reduced sentences.

Maya compiled her final report to the Cascadia School District. It was comprehensive and devastating. It detailed the contract violations, the hidden systems, the data processing, the distribution network. It was the kind of report that would be useful in litigation and federal investigation. It was the kind of report that would stand up to expert challenge because it was built on data and logic and careful analysis.

She submitted the invoice with the final report. Under "Scope of Work," she had written: "Comprehensive data audit with findings of unusual scope. Rate: $400/hour. Hours: 120. Total: $48,000. Payment terms: Net 30. Note: Recommend hazard pay for psychological impact of discovering the dystopian nature of modern educational software. Suggest donation of equivalent amount to organization defending student privacy."

Priscilla approved the invoice and paid it.

Maya sat at her desk that evening with Euler on her lap, looking out at the Seattle skyline. The rain had stopped, leaving everything wet and reflective. The city lights bounced off the pavement below. Cars moved through the streets in the evening pattern. People were leaving work, heading home, settling into their evenings. Somewhere in those homes, parents were not yet aware that their children's behavioral data had been profiled and sold. By tomorrow morning, they would be aware. The news would break. The story would spread. The thing that had been hidden would be hidden no longer.

Tomorrow she would run again, back through the green belt and along the pond. The pattern would continue. But something had shifted. She had found the hidden thing. She had made it visible. She had done what she was good at.

It was not a solution. It was not a fix. It was not justice. The case would take years. Some people would face consequences. Others would escape. The data that had been stolen was still stolen. The infrastructure that had been built would take a long time to dismantle. The children whose profiles had been created would grow up knowing that their behavioral patterns had been analyzed and sold without their consent. That knowledge would change them, would make them suspicious of systems that claimed to serve them. It would make them understand, at a deeper level than they should have to understand,

that institutions could betray them.

But the hidden thing was hidden no longer. The system that was designed to work in darkness was now operating in light. The beauty of that system, the elegant architecture that connected data to knowledge to influence to profit, was now exposed to scrutiny. And scrutiny would break it. Not immediately. Not completely. But enough.

The case would not end perfectly. The justice would be partial. Some wrongs could never be fully righted. But the hiding would be disrupted. The flow of data would be halted. The algorithm would be shut down. The secondary pipeline would be dismantled.

And that change, however small, however temporary, was the work that Maya Chen did. It was enough. She understood that enough was all you could ever really get.

The Witness

Agent Webb arranged for Maya to provide a formal witness statement in his office. She brought Tomás with her, technically as her attorney, though Tomás was not sure that he actually needed to be there since Maya was testifying about her own investigation, not defending herself against anything. But Maya had asked him to come, and Tomás had agreed without making her defend the request.

"This changes things," Tomás said as they drove to the FBI field office in downtown Seattle. The morning traffic on I-5 was thick with the usual commute, and Tomás drummed his fingers on the steering wheel in the kind of rhythm that meant he was working through something in his head. "Once you give a statement to federal investigators, you're part of the investigation. You're a witness. You could be subpoenaed."

"I know," Maya said. She was watching the office buildings accumulate on the horizon, the downtown core growing larger, and she noticed how the light this morning was the particular gray-white of Seattle in early summer, all the sharpness leached out of things. She had been expecting this conversation.

Tomás was the kind of person who needed to talk through the implications before they happened. He was methodical about risk, which was why he was good at his job and also why he frequently annoyed her with lists of worst-case scenarios.

"You could be required to testify in a trial if there is one," Tomás said. He was still drumming, building toward something. "You could be deposed. You could be cross-examined by attorneys who are specifically trying to make you look like you're making this up or that you're biased or that you misunderstood what you found." He had that particular lawyer-voice, the one that was delivering information in a sequence that was designed to allow her to process each piece before the next one arrived. "You could face discovery requests asking you to produce all your work product. You could be asked questions about your methodology that you might not have good answers for."

"I know," Maya said. Her hands were steady on the wheel. She had been through enough professional scrutiny to understand that public testimony was different from having her work reviewed by other experts. Public testimony meant having her conclusions attacked not on their merits but on any vulnerability that could be manufactured.

"This is not a consulting contract anymore," Tomás said. He was choosing his words more carefully now, which meant he was moving into the territory he really wanted to talk about. "This is something more complicated. This is federal. This is real."

"I know," Maya said. "But this is what needs to happen."

The FBI field office was in a building that looked like an office building, which was the point. No one expected the FBI to look like anything in particular anymore. It was on the eighteenth floor of a mid-rise downtown, the kind of place where office suites were clustered behind frosted glass doors with minimal signage. Agent Webb met them in a conference room that smelled like coffee and the particular staleness of rooms where windows did not open. The conference table was the kind of generic furniture that could have been in any office in any building. There was a recording device positioned at the center of the table.

"I'm recording this for accuracy," Webb said. He looked different in this setting than he had looked at the district office weeks ago. More official. More careful. He set up a recording device and tested it with a few sentences. "Is that acceptable?"

"Yes," Maya said. She had been through enough depositions in her forensics work to know that being recorded was standard and that objecting to it would only make things more awkward.

Webb walked her through everything. The initial contract audit that had seemed routine. The discovery of secondary processing systems that did not appear in official documentation. The identification of Project Cornerstone, the careful isolation, the separate infrastructure. The tracing of the corporate structure through shell companies and consulting relationships. The identification of data recipients. The financial flows that proved money had moved in exchange for data access.

She walked through it methodically, organizing the narrative around discovery. Here is what I found. Here is how I found it. Here is what it means. This was the methodology she had learned in her MPSA Analyst ribbon training, the structure of laying out evidence so that the chain of reasoning was visible, so that someone could follow her thinking even if they did not understand the technical details. She was applying the Analyst's forensics methodology to corporate fraud, treating Axiom's infrastructure the way she would have treated a crime scene: cataloging, sequencing, drawing inferences from patterns.

As she talked, she watched Webb's face for signs that he understood the scale of what Axiom had done. Most law enforcement agents, in her experience, did not have a deep understanding of data systems. They understood crime, they understood fraud, they understood the legal frameworks. But the specific mechanics of how a behavioral profiling system worked, how the data flowed, how the vulnerability was constructed, often required additional explanation. Webb seemed sharper than most. He asked clarifying questions about the database schema. He asked about the isolation of the secondary system, why it mattered that it was documented separately. He asked about the financial flows and why that was evidence of intent.

"How can you be sure that this profit motive was explicit?" Webb asked. "How do you know it wasn't just internal analytics that someone decided to monetize only later?"

"The infrastructure was built from the beginning to isolate this data," Maya said. She was walking through her evidence the way she had walked through it a hundred times in her own analysis. "A company that wants to do internal analytics builds systems that are accessible to engineers and product teams. A company that wants to hide something builds systems that are deliberately difficult to access, that are documented separately, that exist in a different part of the organizational chart. Axiom built the second kind of system."

Webb nodded. He understood the inference. "I need to interview her," Webb said when she mentioned Delia Park. "She's the person with inside knowledge. She's the one who can testify about what was actually happening at Axiom."

"She's willing," Maya said. "But she needs protection. She took significant personal risk." Maya had thought about Delia over the past weeks. Delia was angry in a way that Maya recognized, the particular anger of someone who had been complicit in something they did not believe in and who had decided, finally, that anger was preferable to compliance. That was a dangerous person to have on your team, but it was also a person you could trust. Delia had burned her own boat.

"I can't promise protection until I understand the full scope of what she accessed," Webb said. "But I can offer her a proffer agreement. She cooperates, she's not prosecuted for any unauthorized access."

"You should offer her more," Tomás said. This was his first contribution to the conversation, and he had been waiting for the right moment. "Offer her immunity for actions taken in good faith to disclose what appeared to be illegal activity. That's the standard for this kind of whistleblower situation."

Webb nodded. He had the expression of someone who had considered this already but who appreciated having it suggested. "I'll draft it."

The formal statement took three hours. They worked through the afternoon and into early evening. By the time she was finished, Maya understood why witnesses in federal investigations felt hollowed out. She had told the story accurately but completely. She had left no room for interpretation or alternative meaning. Everything was laid bare: the technical details, the financial flows, the careful documentation she had assembled. It all felt smaller when stated aloud than it had felt when she was tracing it through the systems themselves.

Webb asked about her sources. She told him about Delia Park and how Delia had accessed the data. She explained what Delia had risked. She walked through the secondary systems, the isolated infrastructure, the data transformations. She explained the difference between anonymized data and data that could be re-identified with sufficient contextual information. She talked about her own methodology, how she had cross-referenced the data outputs with the financial records, how she had traced the money to identify the recipients.

"So you're confident about the data recipients," Webb said.

"I traced the money," Maya said. "The money went to shell companies. The shell companies received data transfers. The shell companies made payments to organizations involved in political targeting and ad tech operations. That's sufficient confidence for me."

"But you didn't personally observe the data transfer," Webb said.

"No," Maya said. "I observed the inputs and outputs. I observed the financial transactions. I did not observe the pipe between them."

Webb made a note. This was the gap in the evidence, the place where inference became necessary. But inference based on careful analysis was still inference.

As she was leaving, Webb said, "I need you to be available as this progresses. We might need additional statements. We might need you to review documents. We might need you to walk through the technical details with other investigators who don't have your background." He handed her a card with his direct number. "Call me if you think of anything else. And call me if anything

seems unusual."

"I understand," Maya said. She was thinking about the time commitment, the disruption to her existing work. She was also thinking about the fact that this was no longer in her control, that the investigation would move at its own pace according to its own logic, and that she had set something in motion that she could not reverse or redirect.

Over the next month, the investigation expanded with the kind of momentum that federal investigations developed once they had evidence and direction. The FBI interviewed employees at Axiom. They interviewed employees at CrossStile Analytics. They interviewed people at American Insights LLC. They interviewed political operatives who had received data from Axiom. They traced the money: which organizations had purchased the data, how much they had paid, what they had used it for.

Maya watched the process unfold through updates from Webb and from Jennifer Park, the AUSA who was building the case. The investigation was following the pathways that Maya had identified in her analysis. They were finding the evidence that supported her initial findings. The scope of the violation was becoming clear, and it was larger than even Maya had initially understood. Axiom had sold profiles on more students than she had initially thought. They had made more money. They had reached more organizations.

Delia Park cooperated with the FBI under a proffer agreement. She testified about the secondary processing systems. She testified about the data schema. She testified about what she had observed in Project Cornerstone. She testified about the conversations she had overheard between Garrett and James Porter about the value of the data versus the value of the educational software. "Garrett said something like, 'The real money isn't in learning outcomes, it's in knowing what kids are vulnerable to,'" Delia had told Maya the week before. "And James just nodded like that was the obvious truth." The FBI offered her immunity in exchange for her cooperation, protecting her from charges related to unauthorized system access.

Garrett Sable lawyered up completely. He retained Richard Chambers, a partner at one of Seattle's most prominent white-collar defense firms, and he

would not meet with the FBI. He made a statement through his attorneys denying any wrongdoing. He claimed that all data processing had been for legitimate educational purposes. He claimed that any perception of contract violations was a result of misunderstanding complex technical systems.

But Garrett had made the mistake of writing emails. The FBI found emails where he discussed the pivot to behavioral profiling. They found emails where he justified it: "The real value is in the data. The educational software is the vehicle. The data is the cargo." He found emails where he discussed pricing the behavioral profiles: "We can get three hundred thousand for a clean dataset of fifty thousand profiles from a single district. Multiply that across a hundred districts and the economics become interesting." He found emails where he expressed confidence that the secondary processing would not be discovered because "the system is deliberately isolated and documented separately. James understands that the architecture itself is our protection."

The case was becoming straightforward. Axiom had violated the contract. Axiom had processed student data in ways that were not authorized. Axiom had sold that data to third parties. Axiom had done this knowingly and deliberately.

The only question was whether it also constituted a federal crime. Webb believed it did. He was building a case around violations of the Children's Online Privacy Protection Act, which regulated how companies could collect data on minors. He was building a case around wire fraud, since the data had moved across state lines. He was building a case around conspiracy.

Maya's role shifted. She was no longer the consultant who had discovered the problem. She was now the expert witness who would explain what she had found to prosecutors and potentially to a jury. Webb arranged for her to meet with the Assistant U.S. Attorney handling the case.

Jennifer Park was a woman in her early forties who had the appearance of someone who had spent years prosecuting fraud and who took considerable personal satisfaction in being right about how systems could be rigged. Her office was organized with the kind of precision that suggested she thought in systems the same way that Maya did, which immediately made Maya trust her more than she trusted most prosecutors. Jennifer had bookshelves full of case

files, organized by year and by outcome. There was a coffee maker in the corner and cups that suggested she spent more time in the office than she spent anywhere else.

"Your analysis is excellent," Jennifer said. She had Maya's full report printed out and marked up with notes. "Walk me through the chain of custody and how you've established that the data actually left Axiom."

"I can't establish that definitively," Maya said. "The data goes into Project Cornerstone. The output is behavioral profiles. Those profiles were definitely distributed to CrossStile Analytics. I have the financial records showing payment. I have the network logs showing the transfer. But whether the raw student data itself left Axiom's servers is harder to prove." Maya had worried about this gap from the beginning. It was the one piece of the chain that relied on inference rather than direct observation.

"The technical experts can work on that," Jennifer said. She sounded confident, and Maya recognized it as the confidence of someone who had worked with forensic investigators before and who knew what was possible with server logs and backup systems. "We have Axiom's servers in custody. They're analyzing the storage systems, the network logs, the backup systems. They'll be able to show data transfer."

"In the meantime," Jennifer continued, "your analysis gives us the roadmap. You've identified the structure. You've identified the relationships. You've identified the recipients. That's what we need to build the prosecution. You've shown us the shape of the crime."

Over the summer, the investigation reached critical mass. The FBI had interviewed over fifty people. They had reviewed thousands of documents. They had traced the money to show that organizations across the political spectrum had purchased Axiom's behavioral profiles. Democrats and Republicans and third-party groups had all been buying behavioral profiles on the same pool of students. The school district data had become a commodity, passed between organizations that wanted to understand population vulnerabilities.

The prosecutor's office was preparing charges. Garrett Sable would likely be charged with conspiracy to commit fraud, wire fraud, and violations of the Children's Online Privacy Protection Act. James Porter would likely face charges for his role in managing Project Cornerstone. Daniel Kim had cooperated with the FBI and was unlikely to face charges in exchange for testimony about the technical architecture.

And Maya was preparing for the possibility of trial, which was still months away but which was becoming increasingly real as an outcome. She had moved part of her consulting business into a holding pattern. She had reduced her hours with existing clients. She had made space in her life for the investigation to continue.

She was sitting at her desk on a Friday afternoon in July, reviewing her analysis for the hundredth time, when she got a call from an unknown number. She almost didn't answer it. But something made her pick up, some instinct that this was important.

"Is this Maya Chen?" a male voice asked.

"Yes," she said.

"This is Garrett Sable. I'm calling you because I want to explain what happened, and I want to do it before there's a trial and I'm speaking through lawyers."

Maya said nothing. She was calculating whether she should be having this conversation, whether she should record it, whether she should end it immediately and call Webb.

"I started Axiom because I genuinely believed that personalized learning could improve education," Garrett said. His voice was different than she remembered it. Smaller. Less confident. "That part was true. But the economics of education software are brutal. Everyone undercuts everyone. You can't make money. So I looked at other applications of the same technology. I looked at behavioral targeting. I looked at what ad tech companies do. And I thought, why shouldn't education software also generate revenue from the data it collects? Everyone else does."

"Everyone else operates in a different legal context," Maya said. She had decided to keep listening. This was him trying to construct a narrative about how he had arrived at his choices, and she wanted to understand how someone convinced themselves to do what he had done. This was anthropology now, the study of how reasonable people arrived at terrible choices.

"I know," Garrett said. "Believe me, I know that now. But at the time, I convinced myself that it was fine. I convinced myself that the data was anonymized. I convinced myself that the behavioral profiling was auxiliary to the educational mission. I told myself a story that made what I was doing acceptable. I believed it."

"And now?" Maya asked.

"Now I'm facing federal charges and my company is destroyed," Garrett said. "And I'm starting to understand that there's a difference between what's legally permissible and what's actually defensible. I'm understanding it because I'm being forced to. But I wouldn't have understood it otherwise."

"Why are you calling me?" Maya asked. She was thinking about how his call had come to her, not to Webb or to his attorney. He was choosing her as the audience for this confession.

"Because you saw what I was doing more clearly than I saw it myself," Garrett said. "And because I want you to know that the thing you were afraid of, the thing your analysis suggests is possible, is actually worse. I only processed students from one district. I only sold the data to political organizations and ad tech companies. But the system could scale. If I had had more success, if more school districts had adopted Axiom, if we had been able to distribute this system more widely, the scope of behavioral profiling would have been remarkable."

"I know," Maya said. She had been thinking about this for months, the exponential nature of the vulnerability.

"Do you?" Garrett asked. "Do you understand what it means to have detailed psychological profiles on hundreds of thousands of children? To know their vulnerabilities, their fears, their susceptibility to influence? To be able to use that information to shape their political beliefs, their consumer preferences,

their self-image? That's the real scope of what I was building."

"Yes," Maya said. "I understand."

"I wanted to stop," Garrett said. His voice had taken on the quality of confession, the relief of finally saying something out loud that had been consuming him. "Somewhere around Series B, I wanted to stop and just be an education software company. But I had investors who wanted higher returns. I had competitors who were already doing similar things. I had a CEO who wanted to be successful, and success looked like growth and exits and returns on investment. So I kept going. I made decision after decision that felt necessary at the time. And the accumulation of those decisions created something that became a different kind of company."

"Are you recording this?" Maya asked.

"No," Garrett said. "And I'm asking you not to mention this call to anyone. I'm calling you for the same reason I'm calling my therapist, because I need to say out loud what I did and I need someone to tell me that I should have known better."

"You should have known better," Maya said.

"I know," Garrett said. "I do now."

He hung up.

Maya sat at her desk for a long time, thinking about Garrett Sable. He was not a villain in the way she had imagined. He was something more complicated: a person who had made a series of decisions that each seemed reasonable at the time and that had accumulated into something monstrous. A person who had told himself stories about what he was doing that made it acceptable. A person who had believed those stories until someone else had forced him to look at what he had actually built.

She made a note of the call in her file, with timestamps and quotes as much as she could remember. She was not going to call the FBI about it, because Garrett had called her, not the other way around. But she would disclose it if asked. In the meantime, she would keep it as evidence that sometimes people understood their own wrongdoing, but only after it was too late to fix it. She would keep it as evidence that the gap between understanding

and action was sometimes measured in years, that understanding did not arrive all at once but in pieces, each piece demanding acknowledgment.

The Deposition

Jennifer Park, the AUSA, wanted to conduct a deposition of Maya before moving forward with formal prosecution. This was technically optional, but it was good practice for complicated cases. It gave the prosecution and the defense an opportunity to establish what the expert witness would actually say, and it sometimes caught problems or inconsistencies that needed to be resolved before trial. It also allowed defense counsel to search for vulnerabilities in the analysis, to find places where a jury might doubt the conclusion.

The deposition was held in Tomás's office on a Tuesday morning in August. The conference room smelled like fresh coffee and the particular smell of carpeting that had been recently cleaned. Jennifer was there with her case files and her organized mind, several thick folders spread in front of her. Garrett Sable's attorneys sent a representative named Richard Chambers, who was the kind of white-collar defense attorney who had probably won cases through sheer force of personality and detailed knowledge of precedent. He was tall, with the kind of posture that suggested he had spent considerable time in courtrooms, and he entered the room with the confidence of someone who had prepared carefully. He was wearing a suit that cost more than Maya's

monthly rent.

Maya sat across from them, and Jennifer guided her through her analysis once more, this time with Richard asking aggressive questions designed to undermine her conclusions. She had expected this. The deposition was a preview of trial testimony, and Richard was treating it as such. He was not attacking her personally; he was attacking the logical chain that connected her observations to her conclusions.

"You found irregularities in the system," Richard said. His manner was cordial but his intent was adversarial, which was the entire point. "But you didn't find the actual transfer of raw student data, did you?"

"No," Maya said. "But I found the processing system that would facilitate that transfer. I found the output distributions. I found the financial transactions that correspond to those outputs."

"You found that the system exists," Richard said. He was methodical, building his argument piece by piece like a prosecutor himself, which of course was his training. "You did not find evidence that it was used for illegal purposes."

"The existence of the system combined with the distribution of profiles is evidence of illegal purpose," Maya said. She was thinking about the structure of the argument from her MPSA Analyst ribbon methodology, about how to present evidence in a sequence that was logically compelling. "A system designed to be hidden, documented separately, and isolated from the main corporate structure, combined with financial transactions that correlate with data distributions, constitutes evidence of intent to conceal the purpose."

"Or it's evidence of a system that was designed but not used," Richard said. He was building his own narrative now. "Or a system that was designed for a purpose that was perfectly legal and you're simply interpreting as sinister because you're looking for wrongdoing."

"What purpose would that be?" Maya asked. She was letting her skepticism show slightly, letting him see that she had considered this already.

"Internal analytics," Richard said. "Axiom could have been using the secondary processing system to improve the learning algorithm. The profiles

could have been distributed internally for product improvement."

"Then why isolate the system?" Maya asked. She was building her own counter-narrative. "Why create shell companies to handle the distribution? Why hide the connections from Axiom's official corporate documentation? Why have James Porter manage a completely separate infrastructure instead of having the primary product team handle the analytics? Why structure it so that fewer than a dozen people knew about the existence of the secondary system?"

"Companies isolate systems for many reasons," Richard said. He was not flustered by the evidence. This was what he did, found alternative narratives that made the evidence ambiguous. "Security. Intellectual property protection. Organizational clarity. None of those suggest wrongdoing."

Jennifer interrupted. She had been letting Maya handle the technical questions, but now she was moving into her own territory. "The shell companies took money. The money came from political organizations. That's in the bank records. I have the wire transfer records. I have the corporate filings. CrossStile Analytics paid American Insights LLC one point two million dollars in the first year. American Insights LLC distributed eighty percent of that to Axiom through consulting fee contracts that describe the payment as 'educational research consulting.' Educational research consulting for what?"

"The money could have been for consulting services," Richard said. He was not flustered by the evidence. This was what he did, found alternative narratives that made the evidence ambiguous. "It could have been for research. It could have been for any number of things."

"Consulting services in what?" Jennifer asked. "What educational research would justify transferring student behavioral profiles to a political organization?"

"That's a question for my client," Richard said. And that was the problem with the case, right there. His client was not answering questions.

The deposition continued for eight hours. Richard had clearly prepared by studying every similar case, every precedent, every successful defense. He asked Maya about her methodology in detail. He asked about her assumptions. He asked about her alternative explanations. He suggested that she had

confirmation bias, that she had been looking for wrongdoing and had interpreted ambiguous evidence as wrongdoing.

"You seem to have an assumption that any company engaging in product improvement would do so transparently," Richard said. "But that's not how tech companies operate, is it? Tech companies have competitive reasons for keeping their algorithms secret."

"There's a difference between keeping algorithms secret and building systems to hide data flows from their primary contracting partner," Maya said. "Axiom was hiding this from the school district that had hired them. The Cascadia School District did not know about Project Cornerstone. They did not know about the secondary processing. That's not competitive secrecy. That's deliberate concealment."

"You don't know what they knew," Richard said. "You know what they said they knew. But internal corporate knowledge and what's written down are sometimes different things."

By the end of eight hours, Richard had established a plausible alternative narrative: Axiom had built sophisticated systems for internal product improvement. Axiom had done some consulting work with political organizations, perhaps to better understand their educational needs or their information needs. There was no definitive evidence that student data had been sold. There was no definitive proof of wrongdoing. He had constructed a reasonable doubt, the kind that a jury might latch onto if they wanted to believe that companies did not actually do these things.

"That was hard, but it was necessary," Jennifer said after Richard left. She was organizing her notes as she spoke, gathering the documents into a file folder with systematic precision. "The jury will hear that argument at trial. You need to be prepared for it." She sounded tired. "You need to think about what additional evidence proves data transfer. You need to think about what answers you would give if he asks the same questions in different ways."

"Can we prove data transfer?" Maya asked. She was thinking about the gap in the chain of evidence, the point where inference became necessary.

"Probably," Jennifer said. She sounded less confident than she had earlier. "The FBI has the servers. They're working on the forensic analysis. But it's slow going because Axiom wiped some of the logs when they realized there was an investigation." Jennifer was frustrated by this, Maya could see it in her jaw. Destroying evidence was consciousness of guilt, and it was also evidence of destruction that was itself a separate crime, but it also meant the direct proof was harder to construct. "They deleted backup copies. They overwrite their disaster recovery systems. But we have some traces in the network logs. We have some artifacts in the storage systems that survived the deletion."

"That's consciousness of guilt," Maya said.

"It is," Jennifer agreed. "But the defense will argue it was routine data hygiene. They'll argue it's standard practice for companies to delete logs after a certain period." She said this with the particular frustration of someone who knew the argument would be made and who knew that juries might believe it.

"How long will trial be?" Maya asked. She was thinking about the time commitment, the months of her life that might be consumed by a trial if one happened.

"If it goes to trial?" Jennifer said. "Probably two weeks. Cross-examination could stretch it longer if the defense wants to attack your methodology in detail. But I think Garrett will negotiate. His attorneys are good, but the evidence is strong. He'll want to make a deal."

"What kind of deal?" Maya asked.

"Guilty plea to some charges in exchange for lenient sentencing," Jennifer said. "Maybe some corporate governance changes at Axiom. Maybe restitution. But his attorneys know the case is essentially over. The only question is how much time he does." Jennifer sounded confident about this, and Maya recognized it as the confidence of someone who had negotiated with defense counsel before and who had a sense of what that counsel was willing to accept.

Two weeks later, Jennifer called with an update. Garrett Sable's attorneys had requested a plea negotiation meeting. Garrett was willing to discuss accepting responsibility for contract violations and data misuse. He was willing to cooperate with the ongoing investigation into other organizations that had

received the data. He was willing to provide evidence about the venture firm that had funded the Series B, about the conversations with investors about data monetization.

The plea negotiation took place in a conference room downtown, one of those windowless rooms that could have been in any building in any city. Garrett was there, looking smaller than Maya remembered him, worn down by six months of investigation. The suit he was wearing was the same kind he always wore, but it hung differently, like someone had let out the seams or like he had lost weight. The intensity was gone. What was left was just a person who had been caught doing something wrong and who was facing the consequences.

Jennifer laid out the charges and the evidence. She explained the likely sentence if the case went to trial and Garrett was convicted. She walked through the emails, the financial records, the testimony from Delia and Daniel and the employees who had observed Project Cornerstone. She showed him the forensic evidence from the servers, the data transfers that had survived deletion. She showed him the receipts from the shell companies, the patterns of money moving from political organizations to American Insights to Axiom.

"If you plead," Jennifer said, "we can work with the court on a sentence that acknowledges your cooperation and your willingness to take responsibility."

Garrett looked at his attorneys. Richard Chambers nodded. Garrett looked at Jennifer.

"I'll plead," he said. "But I want to explain what happened. I want the court to understand how the decision got made. I want to cooperate fully with any investigation into the broader ecosystem."

"That's helpful," Jennifer said. "And it will be taken into account in sentencing recommendations."

The formal plea agreement was worked out over the next month. Garrett agreed to plead guilty to three counts of wire fraud and three counts of Children's Online Privacy Act violations. He agreed to cooperate with federal prosecutors and the FBI. He agreed to provide all documents and testimony

related to Axiom's operations. He agreed to restitution to the Cascadia School District in the amount of seven million dollars, the full contract value. He also agreed to a substantial fine to the federal government, which would go toward victim compensation.

He agreed to something else: he agreed to publicly acknowledge wrongdoing. His attorneys had negotiated this carefully with Jennifer. Public acknowledgment was unusual in corporate fraud cases; typically, defense counsel wanted to protect their client's reputation. But Garrett wanted it. He wanted to make a statement about what had happened at Axiom and why.

The statement came out on a Friday in September. It was published in the Seattle Times and picked up by national media. Maya read it three times before it fully registered.

"I started Axiom Learning Solutions believing that I could improve education through technology," Garrett wrote. "But I made a series of decisions that transformed the company into something very different from what it was intended to be. I allowed myself to be persuaded by venture investors and by my own rationalization that behavioral data collection and sale was acceptable because everyone else was doing it. I was wrong.

"I built a system that collected detailed psychological profiles on thousands of children without consent or disclosure. I built a system that sold that data to organizations that wanted to use it for influence and persuasion. I built a system that was designed to be hidden, that was designed to obscure what it was actually doing. I made decisions at every stage to deepen that concealment.

"I take responsibility for those decisions. I take responsibility for the harm they may have caused. I regret deeply that I allowed myself to rationalize something that I should have recognized as fundamentally wrong. I understand that my regret does not erase the wrongdoing. I understand that my guilty plea does not undo the violation of trust that occurred.

"I am cooperating fully with federal investigations into the broader ecosystem of behavioral data collection and use. I am working with prosecutors to ensure that all facts about Axiom's operations become clear to the public, to

the regulatory agencies, and to the courts.

"This is not a redemption story. This is not about me learning a lesson and moving forward. This is about accepting responsibility for having built something harmful and being willing to face consequences for that choice."

The statement was widely praised for its directness and acknowledgment of wrongdoing. It was also criticized as insufficient. People had lost jobs. Students had been violated. A company had grown wealthy off information that should have been protected. No amount of public contrition could undo that. Some of the advocacy groups working on student privacy issues said the statement was performative, that it was designed to make Garrett look better to a jury or a judge.

Maya read the statement twice. She found herself thinking about Garrett's call in the summer, about the moment when he had said out loud what he had done and acknowledged that he should have known better. He had called her because she was the one who saw what he was doing, because she had forced him to see it. Now he was trying to make that seeing public, to acknowledge it in a way that the whole world could witness.

She did not feel sympathetic to him. She felt something more complicated: recognition that he had chosen wrong and had only understood that choice after it was too late to unmake it. She also felt recognition that he was trying to do what he could now, which was not much, but which was something. He was cooperating with the investigation. He was taking responsibility. He was acknowledging the scope of the harm.

Tomás called her when the plea agreement became public.

"This is mostly over," he said. "Garrett will plead. The trial will never happen. You won't have to testify in court." He sounded relieved.

"What about the broader investigation?" Maya asked.

"That's ongoing," Tomás said. "But you're no longer the focus of it. You're the witness who found the thing. Now the FBI gets to find all the other things that connect to it." He sounded like he had been carrying anxiety about her testifying at trial, she realized. He had been worried about her facing Richard Chambers for days of cross-examination.

"What's the timeline?" Maya asked.

"Could take years," Tomás said. "Federal cases usually do. But the initial work is done. You can move on."

She tried to move on. She returned phone calls from clients who had been waiting. She started new contracts. She rebuilt the steady rhythm of her life: morning runs, work, coffee, evening reading.

But something had shifted. She had looked into the infrastructure of how behavioral data was collected and used. She had seen how easily systems could be built to extract that data. She had seen how little transparency existed around what happened to the data once it was collected. And she had seen that the legal and regulatory systems moved much slower than the technology moved.

It made the morning runs feel different. It made the steady rhythm feel like a version of ignorance, the kind where you could go about your normal life without thinking about the larger systems that were being built around you. She had learned too much. She could not unhear what Garrett had told her, could not unsee the scope of what he had almost built. And she could not stop noticing the patterns in other systems, the signs of things being hidden, the infrastructure of concealment.

The Aftermath

The Cascadia School District held a community forum in October to discuss the Axiom contract breach and what it meant for student privacy protection. The forum was held in the high school auditorium and was packed with parents and community members and media. The auditorium was the kind that smelled like every high school auditorium, some mixture of old carpet and furniture polish and the particular staleness of a space that was not used every day. There were news cameras set up in the back. There were reporters from the Seattle Times and the Puget Sound Business Journal. The energy in the room was the particular energy of people who had just discovered that someone had been treating their children as data sources without their knowledge or consent. It was anger held carefully in check, waiting for official language to name what had happened.

Priscilla Holt gave a presentation about what had happened: the contract, the audit, the discovery of irregular systems, the response. She explained the district's decision to suspend the contract immediately and to work with federal law enforcement. She was standing at a podium in front of slides that outlined the timeline and the scope of what had been discovered. She was being careful

and thorough, laying out information in a sequence that made the problem visible to people who had no background in data systems.

She also gave credit. "The discovery of these irregularities," she said, "was made possible by an independent consultant who recognized what appeared to be routine data processing problems and traced them to something much more serious. I want to acknowledge that consultant for her diligence and her willingness to follow evidence wherever it led."

The consultant in question was sitting in the audience, trying not to be obvious about it. Maya had come because she wanted to see how the community responded to the discovery, what they understood and what they did not understand. She was in the back row, next to an empty seat, trying to be invisible. She had not expected Priscilla to acknowledge her by name. Priscilla had not acknowledged her by name, which was smart.

After the presentation, there were questions. A parent asked about whether other school districts should be suspicious of their own contracts. The answer was yes, they should be. Another parent asked whether there would be additional security measures. Priscilla explained the data governance improvements that were being implemented. A teacher asked whether there would be additional training for administrators about data governance. The answer was yes, there would be. Priscilla committed to developing training modules for all district leadership.

An older man stood up. He had the kind of intensity that suggested he had been thinking about this question for weeks. "I want to know what happens to the data that's already been collected," he said. "Axiom said they'd delete it, but how do we know they actually did?"

"The FBI is working on that," Priscilla said. She was choosing her words carefully, being honest about the limitations of what could be proven. "They have Axiom's servers. They're conducting forensic analysis to determine what data still exists and what has been deleted. The process is ongoing, and it's complicated because Axiom deleted some records after they became aware of the investigation."

"And meanwhile?" the man asked. He was pressing, unsatisfied with the answer. "Meanwhile my kid's data is out there somewhere?"

"Meanwhile," Karen Park said from the side of the stage, "we're working with parents and the district to understand the scope of what data was collected and what it was used for. We're filing requests with the FTC to investigate Axiom. We're working to establish new policies for data handling at the district level." Karen was one of the district's lawyers, and she had the particular precision of someone trained to speak carefully in public settings. "We've created a registry of all data requests. We're reviewing what information we've provided to any vendor in the past five years."

Maya listened to all of this and thought about the gap between knowing that something is wrong and being able to fix it. Axiom would face legal consequences. Garrett Sable would serve time. The data that had been collected would eventually be identified and hopefully, at some point in the future, deleted. But the students whose profiles had been built, the families whose information had been violated, would not get to unhave that violation. The understanding that had been generated about them would not be unmade. That knowledge was permanent. Somewhere in whatever storage systems still existed, somewhere in whatever backups Axiom had not been able to destroy, there was a database that contained detailed psychological profiles of 38,000 children. Some of that data would be found. Some of it would be deleted. But the fact of its existence would never be unmade.

Maya was thinking about the students specifically. There were students in elementary school who had had their attention patterns recorded. There were students in middle school who had had their emotional responses analyzed. There were high school students who had had their vulnerability to influence assessed. The data had been collected and sold without their knowledge. The understanding of them had been used by people who did not have their best interests in mind. And there was nothing that would make that unhappened. The violation would persist as a fact even if every byte of data was destroyed.

The real consequence was institutional change. Slowly, school districts across the country would strengthen their contracts. Slowly, lawyers would learn to ask harder questions about secondary data processing. Slowly, the

vulnerability that Axiom had exploited would be closed off. But it would take time. And until it was closed, other companies would find similar vulnerabilities and exploit them. The economy of behavioral data was too profitable. The incentives were too strong.

After the forum, Priscilla pulled Maya aside. They stood in one of the hallways off the main auditorium, away from the crowd. There was a poster about the district's new diversity initiative. There was a poster about a school fundraiser. There was a bulletin board with student art from the various elementary schools. There was the ordinary life of the institution, continuing underneath the crisis. The hallway had that particular institutional quiet that comes after a large meeting, the atmosphere of something significant having just occurred but not yet being fully processed.

Priscilla looked tired. She had been superintendent long enough to understand the scope of what had happened, long enough to understand the implications for the district, long enough to understand that this would define her tenure in some way. She had probably spent the forum processing the fear in the room, understanding what parents were worried about, thinking about how to build confidence that the district had things under control. But she also looked purposeful, like someone who had decided that if a crisis was going to define her tenure, it might as well define it in the direction of better practices. Maya recognized the look because she saw it in the mirror sometimes: the look of someone who had decided that the only way forward was through, that there was no going back to the way things were before.

"I've been thinking about something," Priscilla said. "The reason I called you in the first place was because something felt off. I was asking myself yesterday why I felt that way. And I think it's because I've been doing this long enough to recognize the signature of something being hidden. The patterns change. The language becomes careful. The organizational structure becomes unnecessarily complex. When someone is trying to hide something, they have to build complexity to create places for the thing to hide."

"You have good instincts," Maya said. She meant it. Priscilla had recognized the problem without data, without proof, based only on the feeling that something did not fit. That was the kind of instinct that prevented disasters.

"I want to do something with those instincts," Priscilla said. "I'm thinking about creating a new position at the district: Chief Data Officer. Someone who understands how data moves through an institution. Someone who understands the ways that systems can be designed to hide things. Someone like you." She was being direct. "I want someone who will ask hard questions about every vendor contract. Someone who will push back when people want to implement systems that feel convenient but that expose data unnecessarily."

"I'm not a district employee," Maya said. She was thinking about what that would mean, the constraints of institutional work, the limitations of being embedded in one organization. She was thinking about the loss of autonomy, the meetings, the bureaucracy.

"I know," Priscilla said. "But would you consider it? Full-time, salary, benefits. You'd work with me to establish data governance policies. You'd review contracts. You'd make sure we don't miss something like this again." Priscilla was offering something that sounded stable and boring and necessary.

Maya thought about it. She thought about the morning runs and the independent work and the freedom of being a consultant. She thought about Euler and her apartment and the kind of life she had built. She thought about the autonomy of choosing her own projects and her own schedule. She thought about the fact that she had always planned to work independently, to maintain control over her own time.

Then she thought about all the other school districts where the same vulnerability was still being exploited. She thought about the fact that Axiom had been able to operate at scale because no one at the districts was systematically looking for the problem. She thought about the possibility of preventing the next Axiom by being in a position to catch the early signs, the way Priscilla had caught them. She thought about Garrett's call, about his acknowledgment that the system could scale. She thought about the tens of thousands of children in other districts whose data could be violated the same way.

"Let me think about it," she said.

But she knew what her answer would be.

Over the next month, Maya wrapped up her active consulting projects. She transferred some ongoing clients to other consultants she trusted. She documented her methodologies and her databases. She prepared to make a transition from independent consultant to institutional employee. She said goodbye to the flexibility and prepared for the constraints. She thought about what she was losing: the ability to choose her projects, the ability to refuse difficult clients, the ability to work in a way that was entirely self-directed. She thought about what she was gaining: a salary, stability, the ability to do deep work in one place, the ability to see the effects of her work over time rather than handing off a report and moving on to the next project.

She did this partly because of Priscilla's offer, which she had accepted. But she did it also because something had shifted in how she thought about her work. Being a consultant meant solving problems for individual clients, one at a time. But some problems were systemic. They required institutional change. They required someone on the inside pushing for better practices, constantly, over time. They required someone willing to be tedious about it, to argue the same point in every meeting, to build the structures that would make exploitation harder. That was unglamorous work. But it was necessary work. And it was work that Maya was finally ready to do.

She called Tomás to tell him her decision. They were having coffee at their usual place, and she could see the surprise register on his face when she told him.

"You're going to work for a school district," he said, sounding genuinely confused. "You."

"Yes," Maya said.

"You hate meetings and bureaucracy," he said. This was true. Maya had spent a career avoiding both.

"I do," Maya said. "But I dislike the alternative more, which is allowing the same vulnerabilities to be repeatedly exploited because no one is systematically looking for them." She was thinking about what Garrett had said to her about scale, about what would have happened if more districts had adopted Axiom. "Every district in the country is probably vulnerable right now.

Every one of them has contracts with vendors that are probably extracting data in ways that they don't understand. And the only way to fix that is to have people inside those institutions pushing for better practices."

"That's noble," Tomás said. "It's also going to be incredibly frustrating."

"Yes," Maya said. "It will be."

"When do you start?" he asked.

"January," she said. "After the new year. It gives me time to transition my client work and to prepare."

"So you have a few months to prepare yourself," he said. "I'd suggest meditation. Or drinking. One or the other."

She did neither. Instead, she spent the fall deepening her understanding of school district operations. She reviewed data governance policies from other districts. She studied how education technology companies structured their contracts. She studied the contracts from districts where problems had been found and the contracts from districts where problems should have been found. She prepared a comprehensive analysis of vulnerabilities in how school districts handled vendor relationships and data access. She was building the framework that would allow her to do the work systematically.

In December, Garrett Sable was sentenced to eighteen months in federal prison. The judge acknowledged his guilty plea and his cooperation. The judge also acknowledged the seriousness of what he had done.

"The defendant built a system designed to exploit the vulnerability of children," the judge said. Her voice was careful and measured. "He collected detailed psychological information on thousands of minors without consent. He sold that information to third parties. He took steps to hide what he was doing. This case represents a failure of oversight and a violation of trust that should concern every parent in this state."

Garrett was remanded into custody immediately. He would serve his time at a federal facility in California. Maya watched the news coverage and felt no satisfaction, only a kind of sadness that it had taken legal consequences to get him to acknowledge what he had done. He had understood before the sentencing. He had understood when he called her. But understanding and

facing consequences were different things.

After the sentencing, Jennifer Park sent Maya a brief email: "Thank you for your work on this. It made a difference."

Maya printed it and put it in a file. Moments where work clearly mattered were rare enough to be worth keeping track of. She would look at this email in difficult moments, would remember that the work had been worth doing.

She spent Christmas with her family in San Francisco. Her parents asked her about the Axiom case and whether she felt satisfied with how it had resolved. She talked about Garrett's sentence and about the investigation expanding to other organizations. She talked about the policy work she was starting at the district. Her mother asked whether she was happy about the job change, and Maya did not have a good answer. She said she was committed to it, which was true but which was not quite the same as being happy about it.

She spent New Year's alone in her apartment with Euler, thinking about the year that was ending and the one that was beginning. She was thinking about what institutional work would feel like, whether she would miss the freedom of independent consulting, whether she had made the right choice. She had never worked inside an institution before. She had always been the person outside, hired to find the problems. Now she would be the person inside, trying to prevent the problems. That was a different kind of work. It was work that did not have the clear ending of a consulting project. It was work that would continue indefinitely, that would require persistence and patience.

But sitting with Euler on New Year's Eve, listening to the city outside, Maya thought that maybe that was the work that mattered. Not the dramatic discovery of a problem but the systematic prevention of problems. Not the single heroic investigation but the accumulation of better practices over time.

On January 2nd, she went to work for the Cascadia School District as Chief Data Officer. She had an office in the administrative building, a small space with a window overlooking the parking lot. It was not a particularly impressive view. It was the view of a working building, of a place where the maintenance staff had parked their vehicles, of the infrastructure of the institution. She had a staff of one, which would likely expand when the budget

allowed, which she would need to expand to do the work properly. She had a mandate from Priscilla to identify and close vulnerabilities before they could be exploited.

On her first day, she sat at her desk and looked at her inbox. There were already seventeen emails requesting her to review contracts with vendors. There were already five requests for data access from external organizations. There were already questions about security and governance and best practices. The work was already there, waiting for her.

She opened the first email and started to read carefully, looking for the signatures of something being hidden, the patterns of something not fitting. This was her training from the MPSA Analyst ribbon, the methodology of reading a situation and understanding what was being concealed through careful observation and analysis. She was applying it to contracts now instead of to crime scenes, but the principle was the same: understand what people were trying to hide and then ask why they were hiding it.

The work would never be done. But it would matter. And for now, that was enough.

The Patterns

Three months into her new role as Chief Data Officer, Maya had reviewed forty-seven vendor contracts and had found irregularities in thirty-two of them. Most were not as severe as Axiom. Most were the kind of small violations that occurred when lawyers did not ask the right questions and vendors relied on the assumption that no one was actually reading the fine print. But patterns were emerging that made her nervous, patterns that suggested a systematic undervaluing of student privacy in technology procurement.

Educational technology companies, as a category, did not like to be transparent about how much data they collected or what they did with it. They used vague language about "learning optimization" and "student success analysis" when they meant behavioral profiling and student vulnerability assessment. They structured their contracts to allow data retention and repurposing far beyond what was actually necessary for the stated educational purpose. They built in clauses that allowed them to sell anonymized data to third parties, and they defined anonymization in ways that made it nearly meaningless. They included provisions that allowed them to use data for "product improvement," which could mean anything from fixing bugs to

building new targeting capabilities.

Maya created a comprehensive database of vendor contracts. She identified common problematic clauses, phrases that appeared across multiple contracts, structures that were designed to create ambiguity. She worked with Karen Park to draft new standard language that protected student privacy while still allowing vendors to operate successfully. She was using her MPSA Analyst ribbon training to structure the policy analysis, laying out the vulnerabilities in sequence, explaining how each vulnerability could be exploited, recommending protections. She applied the Operative Mindset Triad -- achieving Clarity about the risks, Control over the contracting process, and Choice in which vendors to work with. She began to require that any new contract include specific provisions about data access, retention, deletion, and third-party sharing. She began to ask harder questions about what "anonymization" actually meant in practice.

Some vendors objected. Some vendors argued that her requirements were too restrictive, that other school districts did not have these kinds of requirements, that it would be cheaper for them to exit the market than to meet the new standards. Some vendors sent representatives to meetings to argue that the data governance was overreach, that it was preventing them from delivering educational value, that they had never had problems before.

"Good," Maya said to Priscilla when vendors complained. They were in Priscilla's office, which was larger and more formal than Maya's, decorated with the kind of art that suggested someone with confidence about what they believed in. "That's exactly what should happen. Let them exit."

"That's harsh," Priscilla said.

"It's honest," Maya said. "If a vendor cannot meet basic privacy standards without arguing that it's economically infeasible, then they should not be doing business with children's data. Let them exit. Let them take their business to districts that don't care about privacy. We'll be safer for it." She was thinking about the vendors who were still operating in ways that violated the spirit of the law, even if they technically complied with the letter of it. She was thinking about the districts without Chief Data Officers, without anyone systematically

looking for the problem.

But not all vendors exited. Some grumbled and negotiated, but ultimately agreed to the requirements because access to a large, urban school district was valuable. They wanted the Cascadia name on their customer list. They wanted the reputation of working with a district that had taken data privacy seriously. Some actually thought the new standards were good practice and incorporated them into their own operations, starting to advertise their privacy practices as a competitive advantage.

By March, Maya had also begun analyzing the data access patterns within the district. How much student data did each school ask for? Who had access to that data? What were they using it for? Were there cases where data access seemed excessive or unusual? She was building maps of data flow, tracking where sensitive information was moving, looking for concentrations of access that did not make sense.

This was harder work because it required looking at practices that existed inside the district, not just policies written by external vendors. It meant asking school administrators hard questions about why they needed certain data, how they were using it, whether it was actually improving student outcomes. It meant being the person in the room who did not accept the obvious explanation, who asked follow-up questions, who wanted to understand the specifics.

Most of the time, she found reasonable explanations. A principal needed data on attendance because truancy patterns correlated with student struggle. A counselor needed data on course selection because course selection could indicate student interest and aptitude. A teacher needed data on assessment results because assessment results indicated whether instruction was working. These were sensible uses of data, the kind of thing that schools should be doing.

But sometimes, she found things that did not make sense. Sometimes she found the signature of something being hidden, the pattern of a question not being asked.

In March, she got a referral from a school social worker named Elena Torres. Elena had noticed something odd in her review of the data that the district was collecting on families in the Newton Elementary school attendance zone. Elena came to Maya's office on a Tuesday afternoon, and she was visibly nervous about raising the issue. Elena was a good social worker, someone who cared about students, and she was worried that she was overreacting or being paranoid.

"We have data on where families live," Elena said when she sat down across from Maya's desk. "We have economic status indicators. We have mobility information. We have family composition. But we're collecting much more of it than we need for educational purposes. It's the granularity of it that's bothering me. It's the detail."

Maya pulled the data request from Newton Elementary. It was filed by the school's principal, Mark Henderson. She had met him once at a district event and had formed the impression of someone competent but not particularly thoughtful about data privacy. He was a decent administrator in the traditional sense; he kept the school running, responded to parent concerns, managed the budget. But he was not someone who thought systemically about the infrastructure of the school.

"What's this data being used for?" Maya asked Elena.

"That's what I wanted to ask you," Elena said. "I asked Mark, and he said he needed it for community outreach. But community outreach for what? We don't do economic targeting. We serve all students regardless of economic status."

Maya called Mark Henderson and asked for a meeting. She made it clear that this was not disciplinary, just a clarification. Mark's office was like every elementary school principal's office: crowded with student artwork and family photos and notices about upcoming events. There was a desk piled with papers and folders, and the walls were covered with thank-you notes and drawings from students. There was the chaotic warmth of a place where children spent their time. Mark himself was a man in his late fifties who had been a teacher before becoming an administrator. He looked slightly nervous about having

been called to a meeting with the Chief Data Officer, which made sense; being called by someone in administrative authority about something you had done was rarely good news.

"I understand you requested detailed economic status data on families in your attendance zone," Maya said. She was sitting across from him, deliberately not at his desk, creating the impression of a conversation rather than an interrogation. But it was an interrogation, really. She was investigating. She was using the same methodology she had used with Axiom, following the chain of evidence, asking questions that seemed open but that actually narrowed the space for acceptable answers.

"Yes," Mark said. "We want to do better community outreach. We want to understand the needs of the families we serve."

"You have that information already," Maya said. "You have enrollment data. You have free-and-reduced-lunch eligibility information. You have home language surveys. What additional data are you asking for?"

"I wanted more granular economic indicators," Mark said. "Income level estimates. Housing stability. Employment data."

"How would that improve community outreach?" Maya asked. She was using the MPSA Analyst technique of asking questions that seemed open but that actually narrowed the space for acceptable answers. She was trying to force him to articulate the actual purpose behind the request.

Mark was quiet for a moment. He was thinking about whether to lie or to tell the truth. She could see the calculation happening on his face. "I was approached by someone from a nonprofit called Community Futures," he said. He was choosing to tell the truth, which was better. "They do community development work in low-income neighborhoods. They wanted data on family economic status so they could target their outreach."

"And you agreed to provide that data?" Maya asked.

"It seemed like a good opportunity," Mark said. "They're doing good work. More resources for our families would be helpful." He sounded genuinely like someone who believed he was helping. The road to hell was paved with good intentions, and Mark had just described his intentions clearly.

"Did Community Futures request that you specifically target low-income families?" Maya asked.

"They said their work was focused on communities with economic need," Mark said.

"So you agreed to collect more detailed data about family income in order to help Community Futures identify low-income families to target with their services," Maya said. She was restating it in clearer language, making explicit what had been implicit. "Is that right?"

"Yes," Mark said.

"And you did this without consulting the district data office," Maya said. She was not asking a question anymore. She was laying out the facts.

"It seemed like something a principal should be able to do," Mark said.

"A principal should be able to do many things," Maya said. "That doesn't mean they should. What you did was facilitate the extraction of sensitive economic data from student records to a third-party nonprofit without explicit district authorization or parental consent." She was being direct because the situation called for directness. If she cushioned the criticism, Mark would not understand the seriousness of what he had done.

"I didn't think it was a problem," Mark said.

"I'm sure you didn't," Maya said. "But there's a difference between good intentions and good practice. Community Futures may be a legitimate nonprofit. But you don't know that for certain. And even if they are, they don't have the right to receive data on the families of your students without explicit authorization." She was thinking about how easily the system could be exploited by someone with bad intentions. Mark had good intentions; Community Futures probably had good intentions. But the infrastructure for exploiting student data had been built anyway, and all it took was one person with a different goal to weaponize it.

She stopped the data transfer immediately. She interviewed Community Futures and found that they were indeed a legitimate nonprofit, but they had been unclear with Mark about what they wanted the data for and how they intended to use it. They had been working on the assumption that the principal

could authorize data sharing. They had not understood that family economic data was sensitive, or that they needed explicit parental consent to receive it. They had made the same mistake that Mark had made: assuming that good intentions were sufficient for good governance.

Maya required that they delete any data they had received and that they return the data request to the district for more appropriate handling. She also required that Mark Henderson complete a training module on data governance and family privacy rights. She was not punitive about it; the training was presented as educational, a way for him to understand the principles that governed data use. But it was also a clear message that this kind of decision-making was not acceptable.

"I feel like I'm overreacting," Maya told Tomás when she described the situation over coffee. They were at a café near her apartment, the kind of place where she had become a regular over the past few months.

"You're not," Tomás said. He was listening carefully, thinking through the implications. "You're catching exactly the kind of thing that leads to larger problems. Someone wants data. They ask someone in a position of authority. That person, wanting to help, authorizes the data transfer. By the time anyone checks, the data is already gone. By the time anyone asks questions, the relationship has been established and it's too late."

"But Mark is a good person," Maya said. "He wasn't trying to harm anyone."

"Good intentions don't replace good governance," Tomás said. "Good intentions plus access to sensitive data often equal disaster. You're preventing the disaster by enforcing the governance."

By April, Maya had restructured the entire data request process. All data requests now went through her office. All requests had to specify the educational purpose. All requests had to go through a review process to determine whether the data being requested was actually necessary for the stated purpose. Any data sharing with external organizations required written parental consent and explicit district authorization. She was building the infrastructure that would make exploitation harder.

Some of the feedback was positive. Teachers appreciated having clarity about what data they could request. Administrators appreciated having guidelines that made decisions easier, that allowed them to say no to inappropriate requests without having to generate those reasons themselves. Parents appreciated knowing that their children's data was being protected, that someone was paying attention. The infrastructure of governance created psychological safety.

Some feedback was negative. Vendors complained that the approval process was slow. Researchers complained that they could not access anonymized data for academic studies without explicit parental consent. Community partners complained that they could not do their work without understanding the populations they served. Schools complained about the administrative burden of documenting their data requests.

Maya was sympathetic to the legitimate concerns. She worked with them to develop approval processes that allowed research and community work while protecting privacy. But she did not compromise on the principle: student data was sensitive. It required careful oversight. It required explicit authorization for use beyond immediate educational purposes.

By May, an interesting thing happened: other school districts started calling to ask how she had structured her data governance. Districts from Portland and Vancouver and Spokane and even Seattle proper asked if she would consult with them. She agreed to a few contracts, working evenings and weekends to help other districts develop their own policies. She was bringing the methodology she had learned at MPSA to bear on the problem, laying out the vulnerabilities systematically, proposing structures that would prevent exploitation.

"You're building a field," Jennifer Park said when they ran into each other at a coffee shop in May. Jennifer had been helping with the federal cases that followed Axiom, and she understood what Maya was doing at a systems level.

"What do you mean?" Maya asked.

"I mean you're taking something that nobody was paying attention to and making it visible," Jennifer said. "You're making other people realize they need

to do the work you're doing. You're creating a standard."

"I'm just doing my job," Maya said.

"Exactly," Jennifer said. "But your job is becoming more visible. Eventually, every school district is going to need a Chief Data Officer. And they're going to look at what you did at Cascadia and copy it. You're setting the template."

That was not why Maya had taken the job. But she recognized it was true. The work she was doing was not just solving the Axiom problem. It was creating a framework for how schools should think about data and privacy.

In June, the Cascadia School District adopted a comprehensive data governance policy that became a model for other districts. The policy included specific provisions about data collection, retention, access, and deletion. It included requirements for parental consent for any data use beyond immediate educational purposes. It included regular audits of data access patterns. It included clear processes for how the district would respond to requests from law enforcement.

Priscilla sent Maya a note: "The board approved your policy without objection. They understand what happened with Axiom. They understand why this matters."

By the end of the year, three other school districts had adopted similar policies. By the end of the second year, that number had grown to twelve. By the end of the third year, the Washington State School Directors Association had begun recommending comprehensive data governance policies to all member districts. Maya was invited to present at the annual conference in Spokane. She was cited in policy documents from other states. She was becoming, despite her best efforts to avoid it, a figure in the field. School administrators called her for advice. Teachers reached out to ask how to implement privacy-first practices. Parents wanted to know how to protect their children's data.

It was slow work. It was frustrating work. It involved endless emails and meetings and negotiations with people who did not understand why data privacy mattered. It involved explaining the same principle over and over to

different audiences, each of whom needed to arrive at the understanding on their own timeline. It involved having meetings where someone argued that Axiom was a necessary lesson the market had to learn. It involved responding to vendors who said her requirements were unreasonable. It involved pushing back against districts that wanted to buy cheap solutions rather than good ones.

But there was something satisfying about the slowness. The work was accumulating. The standard was shifting. What seemed radical now would become normal in three years. That was how institutional change worked. Not through dramatic revelation but through the slow accumulation of better practices.

But it was also work that prevented harm. It was work that gave children and families more control over their own information. It was work that made exploitation harder and oversight easier.

And every time Maya got an email from another district saying they wanted to implement the same policies, she thought about Garrett Sable's call and about the moment when he had acknowledged that he should have known better. She thought about the students whose profiles had been built without their knowledge. She thought about the families whose information had been violated. She could not undo those violations. But she could make them less likely in the future. And that was something. That was the work of prevention, the tedious unglamorous work of building systems that made wrongdoing harder.

The Question

In July of her second year as Chief Data Officer, Maya received an unexpected email. It was from Daniel Kim, the CTO of Axiom Learning Solutions, the person who had cooperated with the FBI and who, as far as Maya knew, had never faced charges. Daniel was contacting her because he wanted to talk about starting a company that did what Axiom could have done if Garrett had made different choices: education technology that was also privacy-first by design. The email was carefully written, measuring his words, clearly anticipating skepticism. The subject line was simply "Building Better" with no other context. She almost deleted it without reading. But there was something about the directness of the subject line that made her open it.

"The technology is not the problem," Daniel wrote. "The incentives are the problem. Companies are incentivized to collect as much data as possible and monetize it through sale or behavioral targeting. I want to build a company where the incentive structure is different. Where the only way to make money is to make a better educational product, not to exploit behavioral data. I know you won't trust me. I don't trust myself. But maybe you could help me build something that makes it structurally impossible to do what Axiom did."

"That's a nice vision," Maya wrote back. "But how do you fund it? How do you convince investors to accept returns based on product quality instead of data monetization? Who would fund a company that explicitly limits how much data it can extract?"

"There's a fund," Daniel wrote. "Impact investors who are interested in technology that does good without extracting value from personal data. I know people who are interested. I wanted to know if you would consider being an advisor."

Maya read the email three times. She was skeptical of Daniel's vision. She had learned skepticism the hard way, through seeing what happened when good intentions met the wrong incentive structure. But she was also aware that unless good people built alternative models, the only model that would exist was the exploitative one. The absence of an alternative did not mean that the exploitative model would be rejected; it meant that it would be accepted as inevitable.

She agreed to have a conversation. They met at a coffee shop in the University District on a warm July afternoon. The café had outdoor seating, and they sat at a small table under a striped umbrella, creating the impression of privacy in a public place. Daniel looked different than he had looked three years ago at Axiom. He looked less confident. More thoughtful. Like someone who had looked closely at what he had built and had decided to build something different. He was also, Maya noticed, thinner, wearing the kind of clothes that suggested he had not been paying much attention to his appearance. His hands shook slightly when he picked up his coffee.

"I know you don't trust me," he said without preamble.

"I don't trust anyone who initially participated in building an exploitative system," Maya said. "Cooperation with law enforcement is good. But it doesn't erase participation."

"I understand," Daniel said. "But I also understand that the way forward is not for everyone who made mistakes to be permanently excluded from participating in solutions. If the only people who can build future technology are people who never participated in building bad systems, then we'll never

have enough people." He was thinking clearly about this, had probably rehearsed this argument multiple times.

"That's an interesting argument," Maya said. "But it assumes that people who participated in bad systems will actually build better systems, rather than just replicating the same mistakes in a new context." She was thinking about how easily systems of exploitation reproduced themselves, how the same incentive structures could corrupt even well-intentioned people.

"You don't have to trust me," Daniel said. "But you could help me build a system that makes it structurally harder to replicate the same mistakes. That's what I want your advice on. How do I design a data architecture that does not allow the kind of extraction and sale that Axiom did?"

"You structure it so that the company doesn't have access to the raw data," Maya said. She was thinking about the principles that would make exploitation structurally impossible rather than just difficult. "You use encryption that the company itself cannot break. You don't store identifying information. You don't create secondary processing pipelines. You don't hide anything. You build transparency into the infrastructure."

"That works for individual privacy," Daniel said. "But educational software needs some data to function. How do I balance functionality with privacy?"

"You don't balance them," Maya said. "You assume they're in tension and you choose privacy every time. If you cannot build the feature you want without compromising privacy, then you don't build the feature." She was channeling her MPSA Analyst ribbon training, the principle of building structural constraints into systems so that certain exploitative choices became impossible. "You make privacy the constraint and you optimize everything else within that constraint."

"That's a strong constraint," Daniel said.

"It is," Maya said. "It's also the only constraint that actually works."

They talked for two hours. By the time they left, Maya had agreed to review Daniel's technical designs and to help him think through the data governance structures that would be necessary to make the system actually

privacy-first instead of just privacy-friendly in marketing language.

Over the next month, she spent hours on encrypted calls with Daniel, reviewing his technical architecture. These were long calls where Daniel would walk through the design and Maya would ask questions. She was not an engineer, but she understood how systems could be structured to hide things, and she understood how they could be structured to prevent hiding. She was looking at Daniel's system with the same methodology she had used to trace Axiom's system: not trying to use it, but trying to misuse it. Not trying to exploit it, but understanding how it could be exploited.

He was building it right. The learning algorithm would work on a local device, not on a central server. This meant that the data never had to leave the student's device unless the parents explicitly approved it. Data would be encrypted in such a way that even the company could not decrypt it. The company would have the key to the encrypted database, but not the key to the student data inside the database. Parents would have control over what data was being collected. They could see exactly what the system was measuring. They could delete data at any time. Teachers would have the ability to use the system without having to surrender student information to a corporate backend. They would have access to the analytics that the system generated, but not to the raw data. The system was designed from the ground up to be privacy-first, which meant that every feature, every algorithm, every interface had been designed with privacy as the primary constraint.

It was technically impressive. It was also technically limiting. The algorithm could not do as much personalization as a centralized system could do. The data could not be used for research or for continuous algorithm improvement in the way that extracted data could be used. The system could not learn from patterns across millions of students because the data never left individual devices. This meant that the system would develop more slowly. New features would have to be designed to work with local data rather than leveraging patterns from millions of students. The learning algorithm would have to be more general rather than perfectly optimized for each demographic subgroup.

But the trade-off was intentional. Daniel understood the constraint and had decided to embrace it rather than fight it. The company would make money by having a better product, not by having more data. Success would be measured by learning outcomes for students, not by how much data had been collected. The business model aligned with privacy instead of being in tension with it. There would be no incentive to collect more data. There would be no incentive to hide how the system worked. There would be no incentive to sell the data to third parties because the company would not have the data to sell.

Maya recognized this as the design principle she had been advocating for: if you structure the incentives correctly, the right behavior becomes the only profitable behavior.

"I want you to invest," Daniel said when the design was complete. They were on a video call, and he was looking directly at the camera, making the request clear and direct.

"I'm not an investor," Maya said.

"You're smart. You understand the problem. You care about student privacy," Daniel said. "You're exactly the person I want involved."

"I work for a school district," Maya said. "I have conflicts of interest. I have institutional constraints. I cannot be an advisor on something and then have the school district contract with that company." She was thinking about the ethics of it, about the appearance of impropriety if nothing else.

"So step back," Daniel said. "Leave Cascadia. Come work with me."

"No," Maya said. "I'm doing important work. I'm not leaving to start a company." She was thinking about the work she was doing at the district, the slow accumulation of changes, the systems being built to prevent exploitation.

"Even if that company could scale the solution you've built at Cascadia to thousands of districts?" Daniel asked. He was pressing, which was reasonable. He was building something important.

"Especially not then," Maya said. "I'm not motivated by scale. I'm motivated by depth. One school district that actually implements good data governance is worth more to me than a thousand districts that have privacy-friendly marketing language." She was thinking about what Tomás had

said about good intentions plus access to data. "I'm motivated by preventing the next Axiom. And the way to prevent the next Axiom is to do the tedious unglamorous work of building governance systems, one district at a time."

"That's noble," Daniel said. "But it's also lazy."

"Explain," Maya said.

"You're criticizing education technology companies for only caring about scale and not about doing the work to implement their systems correctly," Daniel said. "But you're doing the same thing. You care about implementing it correctly at Cascadia. You don't care about helping other districts implement it. You don't care about scaling the approach." He was building his own argument, which was fair. She had been inconsistent.

"That's not fair," Maya said. "I consult with other districts. I share what I've learned."

"In your spare time," Daniel said. "While I'm proposing to make it your full-time work. I'm proposing to build the technology infrastructure that makes it easier for every district to implement privacy-first practices." He was making the case that scale and depth were not incompatible, that you could do the deep work of implementation while also reaching more people.

She thought about that for a long time. She thought about what she had learned working at Cascadia. She thought about the limitations of doing the work one district at a time. She thought about the possibility of building technology that could actually prevent the kind of data extraction that Axiom had engaged in.

She also thought about the possibility of failure. She thought about the possibility that the impact investors would lose interest. She thought about the possibility that Daniel's vision would prove too constrained to be viable. She thought about the possibility that she would leave the district and the new person they hired would undo all the work she had done. She thought about the risk that Daniel, despite his good intentions, would eventually face the same pressures that Garrett had faced, the push toward monetization and growth.

In August, she told Daniel her answer: "I'm not going to invest. I'm not going to leave the district. But I'll continue to advise for no fee. I'll help you

build something that works. And I'll use the work we're doing at Cascadia as a testing ground for the technology you're building. I'll pilot it with a school. I'll give you feedback. I'll help you prove that privacy-first is viable. And I'll do it because I care about the outcome, not because I have a financial stake in it."

"Why?" Daniel asked. "You could make a lot of money if you invested early. You could be part of something that changes the entire industry."

"Because I think you're right," Maya said. "Because I think the only way to actually fix this at scale is to make it structurally impossible to exploit student data. And because I think the best way for me to help is to stay in the district and use the policy work we're doing as a testing ground for the technology you're building." She was thinking about what Garrett had said to her about scale, about what would have happened if Axiom had reached more districts. She was thinking about the fact that the only way to prevent that was to build alternative infrastructure, not to hope that existing infrastructure would improve. "You need someone inside a school district who understands the problem and who can work with you to make sure the technology actually solves it. That's what I can be."

"That could take years," Daniel said.

"It will take years," Maya said. "But that's fine. If the work is worth doing, it's worth doing slowly."

Over the next six months, Daniel built a prototype of the new system. He worked with Cascadia School District to pilot it at one elementary school. Newton Elementary, the same school where Mark Henderson had tried to extract family economic data, the school where Elena Torres had first noticed something wrong. It was the right choice symbolically and practically. Maya reviewed the technology and the governance structure. She made recommendations about how the system should integrate with district practices. She tested the encryption models. She verified that the system was actually doing what it claimed to do. She had become the person who verified, who asked the hard questions, who looked for the hidden exploitations. She was applying the MPSA methodology to technology now, the rigorous questioning, the attention to detail, the assumption that something might be hidden and the

determination to uncover it.

Daniel sent her weekly reports. He showed her the architecture. He explained the cryptographic protections. He walked through the data flows. She found vulnerabilities in the early versions, places where data could be accessed, places where the encryption was weaker than he thought, places where user interface design could leak information. Each time she found a problem, he fixed it. Each time she asked a hard question, he had an answer. He was building this system to withstand her scrutiny, and she was providing it with care and rigor.

By January of the third year, they had a working system that was being used by 200 students at Newton Elementary. The pilot had expanded gradually, carefully. Teachers had time to learn the system. Parents had time to understand what data was being collected. There was no pressure to scale quickly, no sense of urgency to reach more students before the system could be attacked. The pace was deliberate.

By May, three additional schools were piloting it. By the end of the year, five schools were using the system. By the following summer, ten schools had adopted it. The growth was slow but steady, driven by word of mouth from teachers who appreciated the system, by parents who appreciated the transparency, by data that showed the system actually worked.

It was not faster than Axiom's system. The algorithm was less personalized. The analytics were more limited. But nothing was being collected that the school did not explicitly need. Nothing was being stored longer than necessary. Nothing was being sold to third parties. Nothing was being used for purposes that had not been approved. The system was slower but cleaner, less powerful but more trustworthy.

Parents understood what data was being collected and had explicit control over what data was being used. Teachers had the tools they needed to personalize instruction without having to buy those tools from a company that was mining behavioral profiles. The system worked because it was designed for the constraints of privacy rather than despite them. It proved that you did not have to choose between privacy and functionality, that you could have both

if you were willing to do the harder work of building them together.

It was a different model. And once you could see it, it was hard to understand why anyone had ever agreed to the Axiom model in the first place. But you could see the answer too: because the Axiom model was easy, profitable, and it worked. It just worked at the expense of children. This model was harder, less profitable, and it worked at the service of children. That was the choice.

The Town Hall

Priscilla Holt announced her retirement in September. She had been superintendent for twelve years. She was 55 years old. She said she was leaving to do consulting work on education governance and because she wanted to spend more time with her family before her kids were in a new life phase. Her daughter was graduating from high school; her son was heading into his senior year of college. She said she wanted to be present for those transitions. She made the announcement at a board meeting, and she did it the right way, giving the board time to search for a replacement, ensuring a smooth transition.

At her farewell event, held in the same high school auditorium where the Axiom forum had taken place three years earlier, she gave a speech about the importance of oversight and institutional courage. The auditorium was packed with staff and community members and students. There were flowers on the stage. Someone had made a video of interviews with people who had worked with Priscilla. Teachers talked about her advocacy for classroom resources. Administrators talked about her willingness to make hard decisions. Community members talked about her commitment to equity.

"Three years ago," she said, "we discovered that a vendor had violated our trust. That discovery was possible because we were willing to ask hard questions and to follow the answers, no matter where they led. Since then, we have worked to build systems and policies that make it harder for violations to occur. We have prioritized student privacy over vendor relationships. We have chosen slower processes over faster implementation when speed would have meant sacrificing oversight.

"I am leaving the district confident that the next superintendent will continue to prioritize these values. I am leaving with the knowledge that the students of Cascadia are better protected because we chose to take data governance seriously."

She did not mention Maya by name. But the implication was clear. When Priscilla left the stage, the audience applauded for a long time.

After Priscilla left, a new superintendent was hired: Dr. James Crawford, who had previously been superintendent of a mid-sized district in Oregon. James was enthusiastic about implementing the best practices from Cascadia. He was also, surprisingly, interested in expanding the data governance work beyond just managing vendor contracts. He understood that data governance was about more than preventing exploitation; it was about using data ethically to serve students.

"I want to use data to actually help students," he said in his first meeting with Maya. They were in her office, and he was looking at the charts and graphs that tracked data access patterns across the district. "Not in the way Axiom wanted to use data. But in ways that are transparent and beneficial. I want to understand what's working in our schools. I want to identify where students are struggling and direct resources to help them."

"What does that look like?" Maya asked.

"I want to identify students who are struggling," James said. "I want to understand the barriers they face. I want to direct resources toward helping them. But I want to do it in a way that's transparent and doesn't exploit them."

"That's harder than it sounds," Maya said. She was thinking about the line between beneficence and harm, about how easily well-intentioned interventions

could reproduce the same patterns of exploitation that Axiom had engaged in. "Using data to help students is good. But using data to categorize students, to sort them, to predict their futures, that's closer to exploitation even when the intent is good."

"Explain," James said.

"If you use data to identify struggling students and you offer them help, but the data is based on factors like race or family income that correlate with systemic disadvantage, you might be reproducing harm while calling it help," Maya said. "If you identify a student as 'high-risk' based on a profile you built from historical data, you might be constraining that student's future options rather than expanding them." She was thinking about how biased systems could hide under the language of intervention.

"So what do you recommend?" James asked.

"Transparency," Maya said. "Any student data use needs to be transparent to the student and their family. If you want to identify a student as struggling, tell them. Ask them if they want help. Don't do it behind their back based on a profile." She was articulating the principle that had emerged from her work with Daniel, the idea that data use had to be conducted with the knowledge and consent of the people whose data was being used.

"That's going to change how we operate," James said.

"Yes," Maya said. "It will."

But James was willing to make the change. Over the next year, Cascadia implemented a new approach to student support: any intervention targeted at a student had to be transparent. A student had to know they had been identified as needing support. A student had to consent to the support. This was a radical change in how schools operated. In most school districts, students were identified as struggling and interventions were provided without their explicit knowledge or consent. Teachers and counselors made decisions about what students needed and implemented those decisions, assuming that they knew best, assuming that informing the student might be counterproductive.

But James and Maya had decided that students had a right to know. That students had a right to see the data that had been used to identify them. That

students had a right to say no.

This had the effect of making the system slower and more administratively intense. It meant that counselors had to have conversations with students about why they had been identified as struggling. It meant going through a specific protocol: here is the data we have, here is what we think it means, here is what we are offering, would you like to accept help. It meant students could say no. It meant that the system could not operate in secret.

It also had the effect of making it less likely that students would be tracked or constrained by historical patterns. A student could say no. A student could see the data that had been used to identify them. A student could challenge the assessment. The system moved at the speed of transparency rather than the speed of algorithmic prediction.

The change was controversial. Some teachers argued that it was less efficient, that students who needed help might not consent to receiving it, that the administrative burden was too high. Teachers who had designed their practice around being able to identify struggling students quietly were suddenly required to have conversations with those students, to explain the data, to ask for permission. They had to give students agency in their own intervention.

But some teachers argued that it was fairer, that students had a right to know when they were being categorized, that the administrative burden was worth the ethical clarity. And over time, something interesting happened: students were saying yes. When they understood that they had been identified as struggling and when they had the chance to consent to help, most of them agreed to it. The consent process was actually building stronger relationships between students and support services. Students felt seen rather than sorted.

In March of the fourth year, Maya got a request from a teacher named Sarah Chen, no relation, who wanted to talk to her about something. Sarah taught advanced placement classes, which meant she had some access to student performance data. She came to Maya's office on a Tuesday afternoon and closed the door carefully behind her. She was nervous, and Maya recognized the nervousness as the nervousness of someone who had noticed something wrong and who was not sure what to do about it.

"I've been looking at the data on which students are recommended for AP classes," Sarah said. "And I've noticed a pattern. The students who are recommended are disproportionately white, disproportionately wealthy, disproportionately from certain neighborhoods."

"Is the recommendation based on assessment data?" Maya asked.

"That's the official reason," Sarah said. "But I'm wondering if the assessment data itself is biased. If we're using assessments that systematically underestimate the abilities of students from certain backgrounds, then recommending only students who score high on those assessments reproduces that bias." Sarah was thinking clearly about the systemic nature of the problem, about how bias could hide inside the infrastructure of assessment.

"That's a fair concern," Maya said. She was thinking about how Maya herself would have been underestimated by biased assessments, how the system would have constrained her if it had had the power to do so. "Have you looked at whether students who were not recommended but who took AP classes anyway did well?"

"That's the thing," Sarah said. "We don't have good data on that. We don't recommend students from certain backgrounds for AP, so they don't take AP, so we never get the data on whether they would have succeeded. We have a missing data problem."

"That's a systems issue," Maya said. "You need to test the assumption that the assessments are predictive. You need to either change the assessments or change the recommendation process to be more inclusive and then measure whether inclusive recommendations lead to different outcomes." She was thinking about how this mirrored the Axiom problem in some ways: the use of data to sort and categorize students in ways that had enormous consequences for their futures. "You need to deliberately do something different and then measure whether it works."

"How do I do that?" Sarah asked.

"You work with the district to design a data study," Maya said. "You propose recommending students from historically underrepresented backgrounds for AP classes. You track their outcomes. You measure whether

they succeed. If they succeed, you change the process. If the disparities persist, you figure out why."

"That's going to reveal a lot of uncomfortable things," Sarah said.

"Yes," Maya said. "But those uncomfortable things are already true. You're just not measuring them. The question is whether you want to know."

Sarah and Maya worked with James Crawford to design a pilot program. Over the next two years, Cascadia deliberately recommended students from underrepresented backgrounds for AP classes. They tracked outcomes. They found that these students succeeded at similar rates to their peers when given the opportunity. Some of them excelled. Some of them chose to drop the class and took other advanced coursework instead, which was also a legitimate choice. The system had been artificially constraining their options, and when the constraint was removed, they made good choices for themselves.

The finding led to changes in the recommendation process. AP teachers began actively recruiting from all backgrounds. The demographics of AP classes shifted gradually over the next few years, not because of quotas but because the system was no longer constrained by biased data.

It was a small example of how data could be used ethically: to reveal bias, to test assumptions, to drive change. It was not data used to exploit or manipulate. It was data used to make systems fairer. It was using the infrastructure of data collection to serve students rather than to sort them.

In May of the fourth year, Maya was invited to give a keynote address at the Washington State School Directors Association conference. The topic was "Data Governance and Student Privacy." She had been invited to speak because of her work at Cascadia, because the policy frameworks she had built had become a model for other districts, because she had become, unexpectedly, someone whose voice mattered in the field.

She talked about Axiom. She talked about the kind of systems that had been built and why they were dangerous. She talked about what Cascadia had learned about protecting student privacy while still using data to improve schools. She talked about the importance of transparency. She talked about the reality that not all technology that works is technology that should be

implemented. She talked about what happened when profit incentives were misaligned with the mission of serving students.

"We have a choice," she said in conclusion. "We can adopt technologies and approaches that are efficient and profitable and that exploit student data. Or we can adopt approaches that are more labor-intensive and slower and that protect student privacy and student agency. We cannot do both. We have to choose."

After her talk, a dozen school districts approached her about consulting on their own data governance policies. Superintendents wanted her email address. Data directors wanted to know if she was available for contract work. She was suddenly in demand in a way she had not anticipated. The work of data governance had become visible, had become a thing that people understood they needed to do.

By the end of that school year, she was working with five different districts, helping them implement policies similar to the ones Cascadia had implemented. Portland wanted to understand the Cascadia model. Vancouver wanted to know how to structure their data office. Spokane was dealing with a situation that reminded them of Axiom and wanted to make sure it did not happen to them. Seattle proper, a much larger district, wanted to scale the approach across their system. Maya found herself building templates, documentation, training materials. She found herself teaching other people how to do the work she was doing.

She was still working full-time for Cascadia. She was doing consulting in the evenings and weekends. She was tired a lot of the time. Her morning runs had become less consistent. She was making notes on documents at dinner. She was thinking about work problems in the shower. She was living the life of someone who cared about what she was doing and who was willing to work hard to do it well. She was not complaining about the exhaustion; the exhaustion was the price of the work mattering. The tiredness was the evidence that she was doing something difficult that actually mattered.

But the work was mattering. Not in the sense of scale, in the sense of changing the entire education system overnight. But in the sense of showing,

district by district, that another way was possible. That you could have education technology that did not exploit students. That you could have schools that protected privacy and still used data to help students learn. That you could move slowly without being negligent, that you could be careful without being paralyzed. That you could do the work right even if it was hard.

Slowly, imperceptibly, standards were changing. District by district, the policies that had seemed radical three years ago were becoming standard practice. The vulnerability that Axiom had exploited was being closed off, not by law, but by the accumulation of better practices. The infrastructure of exploitation was being replaced by the infrastructure of governance. It was not fast. It was not dramatic. But it was real.

Slowly, imperceptibly, standards were changing. District by district, the policies that had seemed radical three years ago were becoming standard practice. The vulnerability that Axiom had exploited was being closed off, not by law, but by the accumulation of better practices. The infrastructure of exploitation was being replaced by the infrastructure of governance.

On a late afternoon in May, Maya was reviewing contracts in her office when she got an email from Tomás. He had gotten married in the spring, to someone he had met while working on the Axiom case, and now he was sending her a photo from his honeymoon in Portugal. They were standing on a bridge overlooking the Douro River. Tomás was smiling in a way that suggested genuine happiness rather than the happiness performed for photographs.

"Thinking about you," the email said. "And how you changed the course of all of this. Hope you're still standing."

She was still standing. She was tired and frustrated and sometimes exhausted by the slowness of institutional change. But she was standing. And the work was still there to be done. There were more districts to consult with. There were more policies to strengthen. There were more vulnerabilities to close. There was always more work.

She typed a quick response: "Still standing. Still working. Good luck with the marriage."

And she went back to her contracts, reading carefully, looking for the signatures of something being hidden, the patterns of something not fitting. She was reading a contract from an assessment company. The contract was careful about language. But there was a clause about using assessment data for research purposes. The research purposes clause was vague. It said the data could be used for "improving educational assessment." But what did that mean? It could mean improving the assessment itself. Or it could mean using the data for any purpose as long as someone called it research.

She sent the contract back with a series of questions. This was the work now. Not the dramatic discovery of a major violation like Axiom. But the constant questioning, the constant pushing back against vague language, the constant insistence that companies be clear about what they were doing and why.

The work would never be done. But it would matter. And for now, that was enough. More than enough. It was everything.

The Temptation

The email arrived on a Tuesday afternoon, and Maya almost missed it. Her inbox was cluttered with contract reviews, district memos, and vendor pitches. But the subject line caught her attention because it was from Daniel Kim, and Daniel rarely emailed about anything trivial. "Offer: Chief Privacy Officer, DKL Holdings."

She stared at the message for a long time before opening it. They had talked about this possibility months ago, over coffee at a place on Capitol Hill, Daniel probing to see if she was restless in her current role. He had planted a seed without pressure. Now he was making it formal.

The offer was substantial. 250K base salary, plus equity with a reasonable vesting schedule, comprehensive healthcare, flexible hours, the full startup ecosystem treatment. The job description was clean and appealing: ensure privacy protection from architectural forward, shape the governance framework for six companies across multiple product lines, hire and manage a team of privacy engineers. All the work she cared about, none of the bureaucratic tedium of dealing with school boards and parent complaints and slow-moving

district politics.

Maya read it three times before she allowed herself to consider it seriously. Then she stood up from her desk and walked down the hallway to the window that overlooked the parking lot below. It was October, autumn in Seattle, and the light had that particular quality of being both bright and somehow resigned, as if the sun had already made peace with the rain that was coming.

She thought about Axiom. She thought about the months she had spent reviewing their contracts, discovering the scope of Project Cornerstone, watching as they collected data on 38,000 students without meaningful consent from families. She thought about that moment in Garrett Sable's office when she had confronted him about the political micromarking pipeline. She thought about how he had rationalized it so easily: "It's the same technology. We help schools personalize. We help other organizations personalize. The data belongs to whoever can use it most effectively."

She thought about Garrett Sable in federal prison now, serving his seven-year sentence for fraud and conspiracy to violate the Children's Online Privacy Protection Act. She thought about how his conviction had felt like victory at the time. Punishment delivered. Justice served. Case closed.

But the Axiom investigation had finished three years ago, and the landscape had not fundamentally changed. Other companies were still collecting detailed data on students. Other venture firms were still funding companies that built behavioral profiling infrastructure. The logic that had driven Axiom was still driving the entire industry. Scale. Growth. Data as the raw material of personalization. The assumption that more data meant better outcomes and that whoever possessed the data had the right to use it however they wanted.

Cascadia School District had hired her to design new governance structures, and she had done that work carefully and methodically. Now the district was implementing privacy-first practices. Teachers were learning to use data differently. Parents were getting clearer information about what was being collected about their children. Students in some classrooms were starting to

understand that their data was sensitive, that they had some agency over it.

That mattered. She could see it mattering every day. A teacher would tell her that it felt different to teach when you weren't thinking of students as data points to optimize. A parent would call to say she appreciated being asked for explicit consent instead of having data collection buried in registration forms. A student would ask why he couldn't delete information about tests he had failed, and then be satisfied with the answer that yes, actually, he could request deletion after a certain period.

But mattering to 14,000 students in one school district was not the same as mattering to the entire landscape. There were thousands of districts across the country. There were hundreds of ed-tech companies. The Axiom case had exposed one company and sent one CEO to prison, but the system that had created Axiom was still operating at full capacity. Every quarter, new companies were being funded. Every month, new data pipelines were being built. Every day, some venture capitalist was deciding that behavioral profiling was a good investment because the market was growing and the regulations were weak and the exit potential was enormous.

Daniel's offer was seductive precisely because it promised to change that math at scale. At DKL Holdings, she could shape how privacy worked across multiple products, multiple markets. She could build architecture that protected people instead of exploiting them. She could do it efficiently, at the company level, rather than slowly and haphazardly across districts. She could actually move the needle instead of spending her days negotiating with vendors and school administrators.

She walked back to her desk and pulled up DKL's website. She looked at their portfolio. Six companies, all in ed-tech. Multiple product lines. Millions of users across thousands of schools. If she could shift how they handled data, the impact would be exponential compared to her work in Cascadia. That was the seductive part. That was the trap.

It was the classic Silicon Valley logic: scale. Efficiency. Leverage. One lever pulled at the right point moves the entire system. It was how founders thought. It was how venture capitalists thought. It was how technologists were

trained to think. Find a problem, build a solution, scale to millions, change the world.

It was also how Garrett Sable had thought.

She remembered the moment during his deposition when she had really understood his rationalization. He was explaining why Axiom had included political targeting in their data sales pipeline, this secondary business line that was not what the core product was supposed to be. "It's not different from any other personalization," he had said, genuinely believing it. She could see it in his face, the absolute conviction that he was not doing anything wrong. "Schools personalize instruction. We personalize instruction and then we help other organizations personalize their outreach. Campaigns want to reach voters with messages that matter to them. Students want learning experiences that matter to them. The technology is the same. The use case is the same. The only difference is scale."

He had believed it completely. That was what had chilled her then and still chilled her now. Garrett Sable was not a cartoon villain twirling a mustache. He was a smart person, a competent technologist, a person who believed he was building good things. He had simply rationalized a harmful system by abstracting away from the actual impact. He had never had to sit with a parent and explain why her daughter's behavioral data had been sold to a campaign targeting voters based on psychological profiles. He had never had to look at a student and say, "When you were in eighth grade, we built a profile of your personality traits and sold it to someone who used it to manipulate you." Distance creates the possibility of indifference.

Maya opened her reply to Daniel and typed slowly.

"The offer is incredible. The work you're doing is important. But I need to think about what I'm saying yes to and what I'm saying no to."

She sent it to his personal Gmail address. Then she pulled out a notebook and wrote down what she would gain and what she would lose. An exercise from her MPSA days, actually, from a class on decision-making under pressure. When you're confused, write it down. Make the implicit explicit.

Gain: scale, the ability to influence multiple companies at once, architectural power, the chance to build privacy into products from day one, focused technical work without district politics, better salary, a team to manage, technical problem-solving instead of organizational friction, the feeling of momentum.

Lose: daily connection to actual students, ability to see impact in real time, relationships with teachers who were trying to do better work, understanding of how policy actually translated into practice, the ability to walk into a classroom and talk to a third grader about their data and actually know what that conversation meant in context, the feedback loop that kept her grounded.

Lose: accountability to the people affected by her decisions.

That was the real difference. That was what the notebook made clear. At Cascadia, she could see when she was wrong. A teacher could push back and say, "Your policy doesn't work in practice because of this reason." A parent could ask a question that forced her to reconsider her assumptions. A student could tell her that the system wasn't working, and she would have to actually respond to that feedback. That loop, uncomfortable and slow as it was, kept her honest. It kept her from floating up into abstraction.

At a technology company, you got metrics instead of feedback. You got monthly reports on compliance, quarterly reviews of privacy architecture, annual audits. You got data showing that your systems were working as designed. But you didn't get to sit in a third-grade classroom and listen to a kid say, "I like this better because it doesn't make me feel like my mistakes are being recorded forever." You didn't get the evidence that mattered.

She closed the notebook and called Daniel.

"I'm going to say no," she said without preamble.

There was a pause on the other end. She could imagine him sitting at his desk in his office overlooking Lake Union, the light coming in from the wrong angle, him looking out at the water while he processed her refusal.

"Why?" he asked finally. "I thought you'd be excited about this. You've said multiple times that district politics frustrate you. This is an escape hatch."

"Because the work I'm doing at Cascadia is harder and slower and less satisfying on a daily basis, but it's more meaningful because it's grounded in actual institutions where students are," she said. "If I move to a company, I'll be abstractly protecting privacy. But I'll be divorced from the actual impact."

Daniel was quiet for a moment. "You could have impact at the company level," he said finally. "You could shape how privacy works for thousands of schools. You could influence the decisions millions of students are affected by."

"I could," Maya said. "But I'd be doing it one step removed. And I'd be operating in a system where the primary incentive is still profit, not student protection. I've seen how that plays out. I've seen it up close. I'm not sure I can change it from inside."

"You don't know that you can't until you try," Daniel said.

"No," Maya said. "But I have a different hypothesis about how change actually works. I think you show it's possible in one place. You make it work. You document what works and why. You make it clear to everyone watching that a different approach is possible. You don't try to scale it through venture capital. You let other people copy you. That's slower, but it's more honest."

She could hear something in his voice that sounded like disappointment. Daniel was the kind of person who believed in scale as inherently good. He believed in the power of platforms and leverage and networks. He believed that building better systems at the company level was the path to real change.

"That's slow," he said.

"Yes," Maya said. "It is."

"And not very ambitious," Daniel added, and there was an edge in his voice now.

"Maybe not. But it's honest. I'm not trying to move an entire industry. I'm trying to show, in one school district, that a different approach is possible. That teachers don't have to feel surveilled by the systems they're using. That students can learn effectively without their every mistake being permanently recorded and profiled."

She hung up the phone and went back to her regular work. There was a contract from a new vendor called Progression Analytics that needed review. They were offering adaptive learning technology that promised to personalize instruction based on continuous performance data. The question was: what data did they actually need? How much of their business model depended on collecting data they didn't need? What was their actual incentive structure? Would they push for more data collection over time, or could they actually be constrained by privacy policies?

These were the questions she spent her time on now. Reading contracts. Looking for hidden data pipelines. Having conversations with people in IT departments about what their systems could actually do. Pushing back on vendors. Supporting teachers who wanted to teach without feeling like data collection was the primary goal.

It was tedious work. It was administrative work. It was the kind of work that would never make headlines or generate venture capital interest or create a billion-dollar company. It was the kind of work that would make you tired and would often feel futile because you would fix one thing and three other things would pop up that needed fixing.

But it was the work that actually mattered.

She ordered Thai food and ate at her desk while she worked through the Progression Analytics contract. She made notes about what data they were collecting and what they claimed they needed it for. She found three data pipelines that looked like they were designed for purposes beyond improving instruction. One of them appeared to be designed to aggregate data across schools to build predictive models of student behavior. That was exactly the kind of secondary use she had seen at Axiom. That was exactly the kind of thing she needed to stop.

She drafted a list of questions for their sales rep. Hard questions. Questions about the secondary processing pipelines. Questions about who had access to the data. Questions about data retention. Questions about whether the data was ever shared with third parties. Questions that would force them to either answer honestly or admit that they were hiding something.

She knew what would happen. The sales rep would claim that the questions were misunderstandings of how the system worked. The company would send technical documentation trying to explain that the secondary pipelines were necessary for the product to function. They would argue that the data aggregation was an essential feature, not a separate business line. They would push back on her restrictions.

She had been through this many times. It was the predictable dance of vendor negotiation. But she had learned to read it. She had learned to see when a company was genuinely trying to balance functionality with privacy, and when a company was just trying to exploit data while maintaining plausible deniability about what they were doing.

That evening, she went to the gym and ran five miles. She pushed the pace hard enough that her legs burned and her breathing came in sharp gasps. She used the time to think through the contract language. She thought about how to write policies that were specific enough to protect students but flexible enough not to make the tools useless. She thought about the line between necessary data collection and exploitative data collection.

It was a line that required judgment. It was not a bright line. It was more like a color gradient, and where you drew the line depended on your values and your priorities. Companies wanted to collect more data because more data made better algorithms. Schools wanted to collect more data because more data meant more detailed understanding of student needs. She had to stand at the line and say: this is enough. More than this is exploitation.

It was a position that nobody was happy with. The vendors wanted more. The administrators wanted more. But the teachers and students and families felt safer with less. They preferred to have their data not recorded than to have it recorded and then misused, no matter what policies said it was being used for.

She showered and drove home to her apartment in Wallingford. Maxwell, her Russian Blue cat, jumped onto her lap the moment she sat down. He was young and restless and demanded constant attention in a way that was the opposite of her previous cat, Euler, who had died five years earlier. Maxwell was nothing like Euler. But he was present, and presence mattered.

She sat in the darkness of her apartment with the cat purring on her lap and thought about what saying no to Daniel really meant. It meant staying in a job where the political dynamics were complicated and the budget was always tight and the vendors never stopped trying to sell her things. It meant staying in an institution where she would probably spend her entire career fighting the same battles over and over. It meant that she would spend decades pushing back, negotiating, implementing policies, training people, dealing with violations.

But it also meant she could see the impact. She could know that the work mattered because she could see it mattering. She could talk to the students in that classroom and know that they felt less surveilled. She could talk to the teachers and know that they felt more trusted. She could look at the policy and know that families actually understood what they were agreeing to.

It meant that when a vendor tried to implement a feature that would violate student privacy, she could say no. When an administrator wanted to use data in a way that was not justified, she could push back. When a student asked for their data to be deleted, she could make it happen.

She texted Daniel: "I made the right choice to stay."

He responded: "For now. But eventually you might feel differently."

"Maybe," she wrote back. "But probably not."

She put the phone down and closed her eyes. Outside, the rain had started. It was the sound that meant October was ending and November was coming, and the long gray season was beginning. It was the sound of Seattle in the fall, inevitable and untroubled.

Maxwell purred on her lap, warm and present, and she sat with that warmth and let herself believe that she had chosen well. She had chosen grounded work over abstract work. She had chosen visible impact over theoretical possibility. She had chosen to stay in institutions and fight from inside rather than to optimize from outside.

It was not the ambitious choice. It was not the choice that would make her rich or famous. But it was the choice that would let her sleep at night. It was the choice that would let her know that the work she was doing actually mattered to

actual people.

The Expansion

The email from the state Department of Education arrived on a Friday morning, and Maya almost deleted it assuming it was another vendor solicitation. But the signature line caught her attention: Patricia Munroe, Assistant Superintendent for Policy. The subject line was simple: "State Data Governance Committee: Request for Service."

The message was formal but warm. The Washington State Department of Education was forming a committee to develop statewide data governance standards for school districts. They wanted representation from school districts that had successfully implemented privacy-first practices. They wanted Maya specifically, based on her work at Cascadia.

The committee would meet monthly for approximately one year. They wanted her to participate in policy development, help draft standards language, and ultimately work with districts on implementation. It was a significant ask. It would require travel to Olympia multiple times per year. It would require writing policy language that would apply to every school district in Washington state, affecting half a million students. If they got it right, the

standards could create a baseline for privacy protection. If they got it wrong, another half million students would be locked into weak standards for years.

She reread the email twice, paying attention to the deadline for response. They needed an answer within two weeks. Patricia had written: "I understand this is a substantial commitment, and we're happy to discuss scope and timing. But I want to be direct about why we're asking: Cascadia's approach is working. Other districts are asking how you did it. We need to codify those practices into a framework that other districts can implement."

That evening, she called Tomas Reyes, who lived in the apartment next to hers. Tomas was an attorney who had become her de facto legal advisor on privacy issues. He had helped her understand the legal landscape when she was investigating Axiom, and they had become friends in the years since. He was the kind of lawyer who understood that law was not separate from practice; it was embedded in practice.

"I'm being asked to help write state policy," she told him over coffee in her apartment. "I'm worried about it."

"Why?" Tomas asked. He was holding her coffee mug, warming his hands, looking out the window at the city.

"Because I understand what works at one district," Maya said. "I don't know if what works at Cascadia will scale to 300 districts with different capacities, different contexts, different political situations. I could write standards that sound good but don't actually work when districts try to implement them."

"That's a legitimate concern," Tomas said. "But it's also an argument for doing the work, not avoiding it. If you don't do it, someone else will, and they might write standards that are worse."

"True," Maya said.

"Also," Tomas continued, "writing standards is different from implementing them. You can build in flexibility. You can phase implementation. You can create pathways for different district sizes and contexts."

"That's harder to do than it sounds," Maya said. "Policy language has to be specific enough to mean something but flexible enough to be implementable. That's the hard part."

"So it's hard," Tomas said. "That's not a reason to say no."

She called Patricia Munroe the next day and said yes.

The first committee meeting was held in Olympia on the first Tuesday of November. The committee room was in the Education Building, third floor, and the windows overlooked the capitol dome. There were twelve of them around the table: superintendents from different regions, two teachers, an education lawyer, a parent representative, a couple of IT directors, a technology researcher, and Maya.

Patricia opened the meeting by laying out the problem. "Student data is a resource that every district is struggling to manage," she said. She was a careful woman, methodical in how she spoke. "We have questions about what we can collect, what we can do with it, who can access it. Different districts are handling it completely different ways. One district has strong privacy policies. The next district over has almost no policies. That inconsistency is creating problems. Companies don't know what to expect. Parents in one district get protection that families in another district don't. We need consistency."

A superintendent from a suburban district nodded. "And we need consistency that protects student privacy, not consistency that maximizes data collection," she said. "That's why we asked Maya to join us."

All eyes turned toward Maya. She felt the weight of expectation settle into the room. These people wanted answers. They wanted her to explain how to fix something that most of them barely understood was broken.

"The first thing to understand," Maya said carefully, "is that this is a values question, not a technical question. Every school has the capacity to collect detailed data about students. We have the technology. We have the systems. We could monitor every keystroke, track every resource a student accesses, analyze every pattern of behavior. That's technically possible. The question is whether we should. And that question is about what we believe students owe to systems and what systems owe to students."

A superintendent from Spokane shifted in his chair. His name was Tom Wagner, and he ran a large district. "But we're not trying to exploit students," he said. "We're trying to help them. We're trying to personalize instruction, understand their needs, give them support."

Maya had heard this argument before. She had made versions of this argument before she understood what data collection actually meant. "I understand," she said. "And that's important work. But the tools that help are also tools that exploit. A system that can personalize instruction by tracking every move a student makes is powerful. It's also a surveillance system. You need to be willing to give up some effectiveness to avoid exploitation."

"What does that mean in practice?" asked Susan Chen, an education lawyer from Seattle.

"It means your policy restricts data collection to what's necessary for instruction," Maya said. "It means you get parental consent before you use data for anything beyond immediate classroom needs. It means you delete data when you don't need it anymore. It means you don't sell it, don't share it with third parties for profit, and don't use it to build permanent behavioral profiles about students."

She paused and looked at the room. She could see the resistance forming. Superintendents were thinking about how to implement this. Teachers were thinking about how restrictive policies would affect their tools. IT directors were thinking about the technical complexity.

"That's going to be expensive," the superintendent from the coast said. His name was Bill Hutchins. "Hiring staff to manage that, implementing new systems, training people."

"Yes," Maya said. "Doing things right usually is expensive. Right now, school districts are externalizing those costs by allowing vendors to collect and use student data without restriction. The vendors profit from that data. The districts get cheaper tools. The students bear the cost in the form of exploitation. A good governance framework internalizes that cost."

She watched Tomas's expression shift. He was thinking about the liability implications. She was too. If a district implemented weak privacy policies and

student data was later exploited, who was liable? The school? The vendor? The parents had a case? These were the questions underneath the questions.

The committee worked for six months. They met once a month in Olympia. Between meetings, subcommittees drafted policy language. Maya participated on the technical standards subcommittee and the governance subcommittee. She also sat in on the legal review.

It was harder than she had anticipated. There was genuine disagreement about what constituted necessary data. A superintendent wanted to collect detailed information about which digital resources students used so he could optimize resource allocation. A teacher wanted to collect information about reading patterns so she could recommend books. A parent wanted to know that her daughter's search history in the library system wasn't being tracked by algorithms that might later target her for behavioral intervention.

In one contentious meeting in February, Tom Wagner made his case again, more forcefully this time. "If we can't track which resources students use, how will we know what's working and what's not? How will we allocate budgets intelligently? How will we understand student needs?"

"You can track aggregate patterns without tracking individual students," Maya said. "You can know that 60 percent of students accessed the digital library without knowing which 60 percent and which specific books each one read. That gives you the information you need for resource allocation without building detailed profiles."

"But the data is so much more useful if we can see individual patterns," Tom said. He was frustrated. She could hear it in his voice. He was not being unreasonable. He genuinely believed that better data meant better decisions.

"Yes," Maya said. "It is. Which is exactly why you have to restrict it. The most useful data is usually the most privacy-invasive data. That's the trade-off."

They broke for lunch after that exchange. Tomas pulled her aside.

"That was good," he said. "You didn't back down, but you also acknowledged his concern. He's not going to change his mind, but you gave other people in the room permission to be skeptical too."

"I don't know if I'm handling this right," Maya said.

"You're handling it better than most people would," Tomas said. "You understand that there are real tensions here, not just good guys and bad guys. You're trying to find a path through the tensions instead of just winning the argument."

By June, the committee had drafted standards. Strong standards. Standards that required:

Explicit data collection policies describing what was being collected and why.

Parental notice and consent for any data collection beyond the minimum necessary for instruction.

Data access restrictions so only people who needed data for their specific job role could access it.

Data retention limits so data was deleted when it was no longer needed.

Vendor accountability with specific security and privacy standards and contractual terms.

Regular audits and transparency reports to parents.

Student agency so students knew what was being collected and could request deletion.

The standards were designed to be implemented in phases, with different pathways for large districts versus small districts. They were designed to be flexible about technology while being specific about principles. They were designed to protect students while still allowing for data use that actually improved instruction.

But they were also expensive to implement. Vendors immediately started lobbying against them. Several education technology companies released public statements saying the standards were too restrictive, that they would reduce effectiveness, that they would make products less useful. One company, Progression Analytics, sent a formal letter to Patricia Munroe saying the standards would increase their operational costs by 20 percent and asking for a delay in implementation.

Tomas reviewed the letter and called Maya.

"This is interesting," he said. "They're not saying the standards are illegal or technically impossible. They're saying they're too expensive. That's different. That's a negotiation."

"But we can't negotiate away privacy," Maya said.

"No," Tomas said. "But you might be able to negotiate about timeline. You might be able to help them understand what the standards actually cost and what they don't cost. Some of what they're saying is legitimate compliance expense. Some of it is just resistance to change."

Maya was invited to respond to the letter. She did an interview with the Seattle Times instead of responding directly.

"Of course they'll drive up costs," she said. "Data governance costs money. Schools have been externalizing that cost by allowing vendors to exploit student data without restriction. That's ending. Schools have to pay for privacy protections instead of having those protections subsidized by the sale of student data. That's the correct cost structure. The fact that vendors don't like it means we're probably doing it right."

The interview got picked up by education news outlets. Suddenly Maya was getting emails from other districts asking her to speak to their boards about privacy. She was getting interview requests from national media about the state standards. She was being positioned as the expert on privacy in educational technology.

She turned down most of the requests. She did not want to be a public figure or a spokesperson. She wanted to be a person doing the work, not talking about the work.

But she did agree to speak to a few other district boards about implementation. She would drive to places like Tri-Cities and Spokane and talk about how Cascadia had implemented privacy protections without destroying instruction quality. She would show teachers data from Cascadia classrooms showing that outcomes had not declined with more restrictive data policies. She would talk to administrators about the liability implications of not protecting student data. She would talk about the possibility of building education technology that worked for students instead of on students.

By the end of the year, ten other Washington State school districts had hired Chief Data Officers. By the end of year two, that number had grown to thirty-five. By year three, it was becoming standard practice. The role she had helped define was now being copied across the state. Districts were asking each other how to implement the standards. Companies were starting to build products that met the certification requirements. The baseline conversation was shifting.

Maya sat in her office one afternoon in late spring of year three, reviewing a contract from a new vendor, and realized something had shifted beneath the surface. The assumptions in the ed-tech industry were changing. Companies were still trying to sell data collection, but now they had to justify it. They had to explain why the data was necessary. They had to acknowledge the privacy implications. They had to be prepared to defend their practices.

It was incremental progress. It was not revolutionary. But it was real, and it was visible, and it was changing how the industry operated.

She texted Daniel: "I think I made the right call turning down the job."

He responded: "Still convinced the district work is more meaningful than company-level work?"

"Yes," she wrote back. "But not for the reasons I thought when I turned you down. Not because of seeing impact in real time. But because being inside institutions means you can shape what institutions value. You can create expectations. You can make it normal to ask privacy questions. You can shift the baseline conversation. At a company, you're building products. In institutions, you're changing culture."

"That's a better answer than you gave me when you turned me down," Daniel texted back.

"I know," Maya wrote. "I'm learning as I go."

That evening, she met with Tomas for drinks. She told him about the email from Daniel.

"He's right, by the way," Tomas said. "About the liability issue. Districts that implement these standards and then have data breaches will be in a much stronger legal position than districts that had weak policies. Your standards are

not just good practice. They're good liability management."

"I know," Maya said. "But that's not why we should do them. We should do them because they protect students."

"Yes," Tomas said. "But it doesn't hurt that they also protect the districts. Good policy does multiple things at once. It protects the vulnerable, it protects the institutions, it makes sense from a legal and technical and ethical perspective. That's what good policy looks like."

Maya looked at the city from the bar window. The sun was setting over the water, and the light was doing that Seattle thing where it seemed to come from somewhere other than the sky.

"I'm worried about what's next," she said.

"What do you mean?" Tomas asked.

"I'm worried that we're solving one problem, privacy in education, and missing the larger problem. The larger problem is behavioral profiling at scale. It's not just happening in education. It's happening in criminal justice, in employment, in consumer targeting. Axiom was just one company in a larger ecosystem."

"Then maybe that's the next work," Tomas said. "But you don't have to do it alone. You don't even have to do it next. You finish what you're doing with education. Other people will work on other sectors."

"That's not how I think," Maya said.

"I know," Tomas said. "That's why I'm telling you. You're going to burn out if you try to change everything at once."

She drank her wine and didn't argue, but she knew Tomas was wrong. She wasn't going to burn out. She was going to keep going because stopping was not an option. Once you understood what was at stake, once you had seen how systems could be exploited, stopping felt like complicity.

But maybe Tomas was right that she didn't have to do it all herself. Maybe there was other work she could do in the margins, while still doing the district work. Maybe she could help Jennifer Park investigate the venture capital ecosystem. Maybe she could understand the patterns better. Maybe she could

use what she was learning in education to understand what was happening in other sectors.

"I'll think about it," she told Tomas.

"That's all I'm asking," he said.

The Inquiry

Two years after the Axiom case had closed, Jennifer Park called. She was no longer an Assistant U.S. Attorney. She had left the prosecutor's office and was now working for the Institute for Data Ethics and Accountability, a nonprofit focused on privacy and technology regulation. The tone of her voice was different now, less formal, more urgent.

"I need to talk to you about something," Jennifer said. "It's related to the Axiom case, but not directly. Can you meet?"

They met at the same coffee shop where they had met years earlier, when Jennifer was still prosecuting the case. Same corner table. Same view of Pike Place Market below. Different coffee, different conversation entirely. Jennifer looked tired in a way that suggested she had not slept well in weeks.

She opened a folder and laid out several documents. Corporate registration documents. Venture capital filings. Press releases. Board minutes from multiple companies. She had the prosecutor's focus on detail, the ability to see patterns in papers.

"I'm reopening some questions about Axiom's investors," Jennifer said. "Specifically, about Cornerstone Capital Ventures, the venture firm that funded their Series B. We never fully investigated them during the case. We focused on Axiom as a company. But I've been looking at what else Cornerstone is funding."

"What do you mean?" Maya asked, though she had a feeling where this was going.

"They're funding a portfolio of companies that all do variations of the same work: behavioral profiling," Jennifer said. She pointed at the documents. "Workplace analytics companies that build comprehensive profiles of employees. How they work, when they take breaks, what websites they visit, how they interact with colleagues. Consumer targeting platforms. Predictive policing software that profiles communities and individuals for likelihood of future crime. Behavioral analysis platforms for prisons that profile inmates for risk of recidivism. All of them built around the same logic: collect detailed data on behavior, build profiles, use profiles for prediction and intervention."

Jennifer laid out more documents. Company names Maya had never heard of. Board interlocks. Shared investors. A pattern of venture capital flowing toward companies that built infrastructure for behavioral prediction and control across domains.

"Are they breaking laws?" Maya asked.

"Some probably are," Jennifer said. "But proving it is hard. Each company is probably technically compliant with whatever regulations apply to their specific domain. But the pattern across them suggests something larger: systematic investment in the infrastructure of behavioral prediction and control. Not accidental. Not incidental. Systematic."

Maya felt something tighten in her chest. This was what she had feared about Axiom. That it was not an aberration. That it was not a mistake or a bad company or a rogue CEO. That it was part of a larger pattern. That there was infrastructure being built to profile and predict and manipulate human behavior across all contexts: education, work, consumption, criminal justice.

"What do you need from me?" Maya asked.

"I need someone to help me understand how these systems work," Jennifer said. "I need someone who can analyze the connections. I need someone like you. Someone who understands the technology and the incentives."

"I'm not an investigator," Maya said. "I'm a school district employee now."

"You don't have to be an investigator," Jennifer said. "You just have to be willing to look at public documents and help me understand what's actually happening. You understand behavioral profiling. You understand the incentives. You understand what gets hidden."

Maya thought about the months she had spent investigating Axiom. The slow accumulation of evidence. The patterns that had only become clear when you looked at the documents in aggregate. The realization that the company's data practices had been systematic, not accidental. The discovery that they had explicitly designed Project Cornerstone as a separate data pipeline, physically isolated from the main product so they could claim the main product did not involve behavioral profiling.

If Cornerstone Capital was doing what Jennifer suspected, if they were systematically funding companies that built behavioral profiling infrastructure, then Axiom was not unique. Axiom was just one example in a larger ecosystem. Garrett Sable was not a bad actor making a mistake. He was a person operating within a system that pushed people toward exploitation.

That was somehow worse.

"Okay," Maya said. "But I need to be clear: I have limited time. I have a full-time job. I can do this in the margins."

"That's all I'm asking," Jennifer said. "A few hours a week. Help me understand what I'm looking at."

Over the next six months, Maya spent her evenings and weekends reviewing the corporate structures of five companies that Cornerstone Capital was backing. She looked at the boards, the management, the data they were collecting, what they were doing with it, who had access to it. She traced the money. She understood the incentive structures.

She did the same work she had done with Axiom: followed the money, tracked the incentives, tried to understand what the system was designed to do. She developed a framework for understanding how behavioral prediction companies made money: they collected data, they built models that could predict behavior, they sold access to those predictions. The more detailed the data, the more accurate the predictions. The more accurate the predictions, the more valuable the product. That was the logic driving the entire ecosystem.

The picture that emerged was not illegal, but it was troubling. Cornerstone Capital was systematically investing in companies that built behavioral profiling infrastructure. They were not necessarily breaking laws, but they were building systems designed to systematically understand, predict, and influence human behavior at scale.

The venture firm's CEO was a man named David Hsu, who had been a successful technology investor for twenty years. He had founded Cornerstone when he realized that venture capital was shifting away from consumer internet companies and toward infrastructure and data companies. Behavioral profiling was a massive infrastructure play. There was enormous demand for prediction across industries. Companies could build defensible competitive advantages through proprietary data and algorithms. The market was global. The growth potential was enormous.

Hsu was not a villain. He was just an investor following the logic of his industry. The logic was simple: identify a large market, find a technology solution, build a company around it, raise capital, scale, exit. Behavioral profiling was a massive market. Companies would pay for any system that could predict customer behavior, employee behavior, criminal behavior. There was enormous demand for this capability. Governments wanted it. Corporations wanted it. The market was basically unlimited.

This was how venture capital worked. This was how technology got built. You identified a problem and a market, you convinced smart people to solve it, you raised money from investors who wanted returns, you scaled, you exited. The question of whether the system you were building was ethical was secondary to the question of whether it could scale and generate returns.

Maya wrote a report for Jennifer that detailed the connections between the companies, the shared investors, the shared technology platforms, the shared vision of what behavioral data could be used for. She documented the pattern. She made it explicit.

"This is a pattern," she wrote in the conclusion. "This is not accidental. This is systematic investment in the infrastructure of behavioral prediction and control. Each company individually might be legal. But together, they are building a comprehensive system for understanding and predicting human behavior across all contexts: education, work, consumer choice, criminal justice. The venture firm is profiting from building that system. The question is not whether they're breaking laws. The question is whether this system, even if legal, should exist."

She sent the report to Jennifer on a Friday evening and spent the weekend feeling sick. She had looked at the patterns. She had made them explicit. She had documented what the venture capital ecosystem was building, and it was not good.

"What do we do with this?" Jennifer asked when they met the following Tuesday.

"You publish it," Maya said. "You use it to raise awareness. You work with regulators to understand whether any of the individual companies is breaking laws. But mostly, you just document what's happening and let people know."

Jennifer published the report on the nonprofit's website. Within a week, it had been picked up by tech press. Within two weeks, it was covered in business news and policy publications. It generated controversy and discussion about the venture capital ecosystem and its role in funding potentially harmful technologies.

Some of the companies in the report responded with statements saying their technology was being mischaracterized, that they were following all applicable laws, that their work was legitimate and valuable. One company, a workplace analytics firm, hired a PR firm to manage the response. Another company, a consumer targeting platform, published a blog post explaining that

behavioral prediction was becoming ubiquitous and that the real question was who got to control it.

David Hsu, the venture firm CEO, gave an interview to a business publication where he pushed back directly. The interview was long, almost 3,000 words. Hsu was thoughtful and articulate, and he made powerful arguments.

"There's nothing sinister about investing in behavioral data technology," he said in the interview. "Prediction and personalization are inevitable in a modern economy. They're how companies serve customers. They're how schools serve students. They're how governments serve citizens. The question is not whether to do this work. The question is whether the U.S. will control its development. If we don't build this infrastructure, other countries will. If we don't develop behavioral prediction technology, China will develop it first and better. So the question is not whether to develop this technology. The question is whether the U.S. will dominate the market."

Maya read the interview three times. It was a powerful argument. It was also a trap. It was the argument that had justified every exploitative system since the beginning of technology. If we don't build it, they will. If we don't do it, we lose. If we don't develop this capability, we cede control to hostile actors. The argument reframed ethics as weakness, privacy protection as risk, regulation as self-sabotage.

It was the argument that worked because it worked. Governments feared falling behind. Companies feared losing market share. Venture capitalists feared missing opportunities. The geopolitical logic was powerful. The competitive logic was powerful. The ethical logic was easy to dismiss as naive.

She called Jennifer.

"He's right about one thing," Maya said. "This is going to happen. If not in the U.S., then somewhere else. If not by venture capital, then by government, then by some other infrastructure. The question is how. And whether we're going to do anything to constrain it."

"What do you think we should do?" Jennifer asked.

Maya paused. She had been thinking about this for six months. She had been reviewing documents, understanding the incentive structures, understanding why people like Garrett Sable and David Hsu made the decisions they made. She had been trying to think through what structural changes would actually work, what would actually constrain the system instead of just punishing individual actors.

"Regulate it," Maya said finally. "Not ban it, but regulate it. Require transparency. Require consent. Require that people know when they're being profiled and can see their own profiles. Require that the systems be auditable. Make it harder to exploit than it currently is. Make the externalities visible so the costs are borne by the companies doing the profiling instead of by the people being profiled."

"That's not going to happen overnight," Jennifer said.

"No," Maya said. "But it's going to happen. You build a system. It works. People use it for bad purposes. Eventually, regulations catch up. The question is how much harm happens before the regulations arrive."

"You could advocate for that," Jennifer said. "You have credibility. You have evidence. You could shape the conversation."

Maya was quiet. It was true. She could probably influence policy conversations. She could probably help shape regulation. She could probably use her position and her expertise to push toward structural change at the policy level. She could testify to Congress about behavioral profiling infrastructure. She could work with organizations like Jennifer's to build the case for regulation.

But doing that would mean becoming a policy advocate. It would mean speaking to legislators, working with advocacy groups, appearing in public forums and on news shows. It would mean shifting her identity from practitioner to expert. It would mean distance from actual schools. It would mean less time with students and teachers and more time with policy documents and political meetings.

"I could," Maya said. "But I'm not going to. I'm going to keep doing what I'm doing: making it hard to exploit behavioral data in one school district. I'm

going to help other districts do the same. And I'm going to hope that by the time regulations arrive, enough people will have seen that a different approach is possible."

"That's a modest ambition," Jennifer said.

"Yes," Maya said. "It is."

But modesty was strategic. It was the difference between being a person who actually changed behavior in institutions versus being a person who advocated for change from outside institutions. One took longer. One was less visible. But one actually worked.

After Maya hung up, she sat in her office and watched the rain streak down the window. She thought about Garrett Sable in federal prison, serving time for the decisions he had made at Axiom. She thought about David Hsu, still operating, still funding companies that built behavioral profiling infrastructure. She thought about all the people working in the behavioral profiling industry who believed they were building useful systems, who rationalized the surveillance as necessary, who saw the data collection as benign.

She thought about the fact that the Axiom case had not changed the industry. It had just changed one company. Everyone else had learned to be more careful, more transparent, more aware of regulatory risk. But the fundamental logic was unchanged. Companies were still building behavioral profiling systems. Venture capitalists were still funding them. The market was still growing.

Someone had to change that logic from the inside. Someone had to show, in institution after institution, that a different approach was possible. Someone had to prove that you could serve people without exploiting them.

She was not a policy advocate. She was not a political operative. She was just a person trying to protect students in one school district. But she knew that doing that work well, doing it visibly, documenting what worked, sharing what she learned, that was how change actually happened.

Three weeks later, David Hsu called her directly. The call came to her office phone, and she almost didn't answer. It could be a scam. But something

made her listen.

"I read your report," Hsu said without preamble. "The one Jennifer Park published. I wanted to talk to you about it."

"Okay," Maya said carefully.

"You're not wrong," he said. "You've identified what we're doing. You've understood the pattern. You've understood that we're systematically investing in behavioral prediction infrastructure. Where you're wrong is in assuming that's inherently bad."

"I didn't say it was bad," Maya said. "I said it was systematic and designed to be hidden and being used in ways that exploit people."

"Some of it is," Hsu said. "But some of it is genuinely beneficial. You know this. You use data at Cascadia School District to help students. That's behavioral prediction and personalization. You're doing the same thing that Axiom was doing, except you're doing it transparently and you're doing it for the student's benefit instead of for profit."

Maya felt her shoulders tighten. It was true, and she hated that it was true. She did use data to personalize instruction. She did build profiles of student learning patterns. The difference was not the data itself. The difference was the incentive structure, the transparency, the consent, the accountability. But Hsu was forcing her to articulate that difference clearly.

"The difference is the incentive structure," Maya said.

"Exactly," Hsu said, and she could hear the energy in his voice, the sense that he had been thinking about this, that he had been wrestling with the same questions. "The question is not whether to do behavioral prediction. The question is what incentives drive the work. I'm investing in companies that have a profit incentive to do behavioral prediction. Some of them will do it well. Some of them will do it poorly. Some of them will do it harmfully."

"So why are you calling me?" Maya asked.

"Because I want to know what it would take to align the incentive structures," Hsu said. "What if I restructured my investments so that the companies I fund are incentivized to develop behavioral prediction technology in a way that's transparent and that benefits the people being predicted?"

"That's a hard business problem," Maya said. "Your investors expect returns. Transparent, ethical behavioral prediction is less profitable than exploitative behavioral prediction."

"Maybe," Hsu said. "Or maybe the companies that are most ethical and most transparent become the ones that dominate, because they have more trust and more users. Maybe transparency becomes a competitive advantage instead of a constraint."

"You could test that," Maya said.

"I am," Hsu said. "I'm considering restructuring the portfolio. Some of the companies I'm investing in, I'm pushing toward more transparency. Some are resisting. Some are willing to change. I'm learning what's possible."

It was a strange moment. She was having a conversation with a venture capitalist about how to align profit incentives with ethical practices. It was not a conversation she would have expected to have. But it was clear that Hsu was genuinely thinking about the problem, genuinely trying to understand how you could build systems at scale without exploiting people.

"The thing you'll learn," Maya said, "is that transparency costs money. It requires hiring people who care about privacy. It requires slower development. It requires saying no to opportunities that are profitable but unethical. Most venture-backed companies won't accept those costs."

"Some will," Hsu said. "And if some will, that's enough to create an alternative model."

"It might be," Maya said. "Or it might be that the transparent companies get out-competed by companies that are willing to exploit more aggressively."

"That's possible," Hsu said. "But I'm willing to fund the experiment."

After the call ended, Maya sat with what had just happened. David Hsu, the head of one of the largest behavioral prediction funding firms, was reconsidering his entire investment strategy because of a report she had helped write. It was not a guarantee that anything would change. It was not a guarantee that he would actually restructure his portfolio or that transparent companies would dominate. But it was a crack in the system. It was a moment where someone with power had been forced to consider whether power could be used

differently.

She called Jennifer and told her about the conversation.

"That's interesting," Jennifer said. "He's not dismissing the concerns. He's engaging with them."

"That doesn't mean he'll change," Maya said.

"No," Jennifer said. "But it means he's thinking about it. And sometimes thinking about it is the first step.

The Question Answered

Delia Park called on a Thursday afternoon. The voice on the phone was warm but purposeful. Maya had not heard from Delia in years. After the Axiom case had concluded, Delia had kept a low profile, using her whistleblower immunity to stay out of legal trouble. She had moved on to other jobs in education technology companies, each one a different attempt to work within the system instead of against it. They had kept in touch sporadically, exchanged emails at Christmas, but the intensity of their partnership during the investigation had faded once the case was over.

"I'm doing something I think you should know about," Delia said without preamble. "I'm starting a nonprofit that helps education technology companies build privacy-first systems. I wanted to see if you'd be interested in working with me."

They met for coffee on a Saturday morning, neutral territory, away from both their offices. Delia was 40 now, older and more confident than she had been during the Axiom investigation. She wore her experience in her posture. She had spent the last five years working in various education technology roles,

watching how companies approached data, how they rationalized practices, how they pushed toward greater data collection and less transparency. She had also seen what happened when people tried to push back. She had seen people fired for asking questions. She had seen technical debt accumulate from misaligned incentives. She had seen engineers quit because they could not stand building systems designed to exploit. She had decided that the best way to make a difference was to help companies get it right instead of helping them deal with the consequences of getting it wrong.

"I've been thinking about what happened at Axiom," Delia said over coffee. The coffee shop was warm and crowded enough that they could talk without being easily overheard. "I've realized that the problem was not that we were bad people doing bad things. The problem was that the system was set up to incentivize bad behavior. We were trying to build a learning tool, but the incentive structure pushed us toward building a data exploitation tool. Everyone involved was smart and well-intentioned. The system just made us bad."

"What are you planning to do about it?" Maya asked.

"I'm creating a certification program," Delia said. She had clearly thought about this a lot. The words came out carefully structured, as if she had given this pitch before, had refined it. "Education technology companies can volunteer to participate. They open their systems to audit. They implement privacy-first practices. They get certified as privacy-first EdTech. We market that certification to school districts. We help companies understand that privacy is a competitive advantage, not a constraint."

"That's ambitious," Maya said. "That's a huge market shift you're trying to create."

"It is," Delia agreed. "But you've shown it's possible at the district level. You took one district and showed that you could protect student privacy without sacrificing education quality. I want to show it's possible at the company level. I want to create a pathway for companies to do the right thing and be profitable doing it."

She paused. There was something else she wanted to say.

"I've been working at companies," Delia continued, "and I've seen what happens when the incentives are wrong. I've seen smart people making bad decisions because the system pushed them that way. I've been that person. I rationalized data collection as personalization. I rationalized behavioral profiling as helping students. I looked at the money being made off of student data and told myself that it was the nature of business."

"And now?" Maya asked.

"Now I can't live with that anymore," Delia said. "Now I see the children whose data is being exploited. I see the families who don't understand what they're agreeing to. I see the teachers who feel surveilled by the systems they're using. I can't rationalize it anymore. So I have to try to change it."

"What do you need from me?" Maya asked.

"First, I need you to help me define what privacy-first EdTech actually means," Delia said. "What are the non-negotiable standards? What are the things a company has to do to get certified? I need someone who understands both the technical and the governance side. Someone who understands what's actually possible versus what's just theater."

"I can do that," Maya said. "I can work with you in the margins. But I can't leave Cascadia."

"I don't want you to," Delia said. "I want you to stay at Cascadia. I want you to use your position to shape which companies get contracted with, so companies have to meet your standards if they want access to the district. I want to create a market incentive for privacy-first practices."

It was a good idea. It was also work that would take significant time and would be frustrating because companies would argue about what the standards should be and would resist implementation. Some companies would claim that privacy-first practices were impossible to implement. Others would complain about cost. Some would hire expensive consultants to argue that the standards were misguided. But if it worked, if enough districts started using certification as a procurement criterion, then the incentive structure would shift. Companies would start building for privacy because they had to, because the market was demanding it.

"Okay," Maya said. "I'll help."

Over the next year, Maya and Delia worked together to develop a certification framework for privacy-first education technology. They met monthly, sometimes more frequently. They reviewed technical documentation from companies. They looked at how data flowed through systems. They examined what was visible to students and parents and teachers. They asked hard questions about what was necessary and what was exploitation. They studied the business models. They understood what practices generated profit.

They developed a framework that included three categories of standards:

Technical standards: data encryption, data isolation so one student's data could not be cross-referenced with another's, no secondary processing pipelines that used student data for purposes beyond the stated educational goal, comprehensive audit logging so every access could be tracked and verified.

Governance standards: transparent data policies that could be understood by parents without a law degree, active consent mechanisms so families knew what they were agreeing to and could meaningfully opt out, student agency provisions so students knew what was being collected and could request deletion, regular audits by independent external auditors, clear data retention policies.

Behavioral standards: companies had to publicly disclose what data they collected, what they did with it, and who had access to it. Companies had to allow for data deletion. Companies had to acknowledge in their policies that student data was sensitive and carried risk of exploitation. Companies had to demonstrate that their incentive structures aligned with privacy protection.

Companies that met all three categories could be certified as privacy-first EdTech. The certification would be displayed on their marketing materials and would be verified by independent auditors. The certification would matter because Cascadia School District announced that any new technology contract would require privacy-first certification. Other districts, following Cascadia's lead, began to do the same.

The first year, two companies applied for certification: Daniel Kim's company, which had always been designed with privacy-first principles, and

one other smaller startup from Portland. Daniel's company easily met the standards. The startup needed to make some modifications but was willing to do so. Several larger ed-tech companies looked at the standards and decided they could not meet them. Their business models depended on data practices that the certification explicitly prohibited. They would have had to fundamentally restructure their companies to get certified.

One company, a large adaptive learning platform called Progression Analytics, tried to negotiate the standards. Their argument was that the standards were too restrictive for statistical modeling. They wanted to be able to aggregate student data across schools to build better predictive models. Delia and Maya looked at their proposal and rejected it. The benefit to the company was clear. The benefit to students was not.

Progression Analytics lobbied hard. They sent letters to school districts saying the standards would reduce product effectiveness. They hired consultants to argue that the standards were based on a misunderstanding of how machine learning worked. They offered to implement a "compromise" approach that was really just a repackaging of their original business model.

But Cascadia School District and the other districts that had adopted the certification program held firm. The certification was the price of entry. If they wanted to sell to these districts, they had to meet the standards.

By year three of the certification program, twelve companies had been certified. Several had restructured their entire data practices to meet the standards. A few had decided that privacy-first practices were not compatible with their business model and had exited the ed-tech space. One company pivoted their product to focus on transparency tools that let teachers see how student data was being used, rather than trying to hide the data pipeline.

Venture capital was slow to adapt, but some investors had started to understand that companies with strong privacy practices had better customer retention, less regulatory risk, and more defensible positions in a market that was increasingly aware of privacy issues. Some venture firms had started to fund companies explicitly because they had privacy-first practices built in. One venture capital firm, not Cornerstone Capital, but another firm, started using

Delia's certification as a factor in their investment decisions.

Maya and Delia spoke together at a national education conference about the certification program. They gave a presentation titled "Market-Driven Privacy: How to Use Procurement to Change Corporate Behavior." The ballroom was full. There were two hundred people in the room, and the energy was focused. This was a conversation people wanted to have.

They talked about what they had learned building the program. They talked about what companies had resisted and why. They talked about what the certification had enabled. Delia showed a slide showing which companies had applied, which had been certified, which had resisted. Daniel's company was there. Three others. A startup from Portland. A nonprofit that had been developed by a teacher collective. Evidence that a different approach to education technology was possible.

"What we've learned," Delia said, and her voice had the confidence of someone who had been proven right, "is that companies can be profitable and ethical. They can use data to improve instruction and still protect student privacy. What they cannot do is maximize extraction of data and also maintain student privacy. They have to choose. The certification program helps them understand that students and families are increasingly aware of the choice, and districts are increasingly willing to pay a premium for companies that choose privacy."

Maya talked about the experience from the district side. "We're a purchasing power," she said. "We have procurement authority. When we say that vendors have to meet certain standards, vendors have to meet those standards if they want our business. That's not regulation. That's the market working. That's incentive alignment. That's what capitalism can do when you align the incentives correctly."

She talked about the resistance they had faced. "One company tried to argue that our standards were based on a misunderstanding of how machine learning works. They said that the models needed access to detailed student data to work effectively. That was true. But the fact that it's true doesn't mean we have to accept it. We said: build your models differently. Or don't. But you

cannot have access to the data if you want to sell to our districts. The company chose not to sell to us. That was their decision. But other companies chose differently. Other companies found ways to build effective systems without exploiting data."

After the presentation, a teacher named Marcus approached them. He was about Maya's age, probably early 40s, and had the demeanor of someone who had been teaching for decades and was tired of being surveilled by the software he was supposed to use. He introduced himself as a high school science teacher from Eugene, Oregon.

"I want you to know," he said, his voice careful and sincere, "that the privacy-first tools have changed how I teach. I used to feel like I was managed by the software. Like every move I made was being tracked and evaluated. I was teaching in a surveillance state. The platform I was using would monitor my pacing, suggest interventions, flag students who weren't progressing on the expected trajectory. I felt like I was managing students instead of teaching them."

He paused. "Now I feel like the software is serving me. I can focus on the students instead of managing the data. I know which students are struggling because I can see them struggling, not because an algorithm told me they were struggling. I can help them in the way I think is best instead of following algorithmic recommendations. I teach better. Students learn better. And I don't feel like I'm being spied on."

That conversation, that acknowledgment from a teacher that the work was making a tangible difference, was exactly why Maya and Delia did the work. It was evidence that the structures they were building were not just theoretically superior, but actually made people's lives better. It was evidence that the work mattered in ways that could not be measured by metrics or scale.

That evening, Maya and Delia went to dinner. They sat in a restaurant overlooking the water, and for the first time in years, they felt like they had won something. Not completely. Not finally. But they had shifted something real.

"I was scared," Delia said over wine. "I was scared that the market would reject privacy-first practices. I was scared that companies would refuse to change. I was scared that the venture capitalists would just keep funding exploitative companies and that my nonprofit would be irrelevant."

"But you did it anyway," Maya said.

"Because I had to," Delia said. "Because I couldn't live with myself if I didn't try. Because I knew it was possible because you had shown it was possible at the district level."

In year five of the certification program, Delia's nonprofit was awarded a million-dollar foundation grant from the Spencer Foundation to expand nationally. Other states were asking to adopt the standards. Other countries were looking at the model. The work was becoming a movement, slow but visible.

Delia called Maya to tell her about the grant. They met for coffee at the same place where they had first discussed the certification program, a small place on Capitol Hill with good light and quiet corners.

"We did it," Delia said. "We actually created something that worked."

"You created something that works," Maya said. "I helped. But this is your vision. This was your idea and your drive."

"It started with your work," Delia said. "You showed that privacy-first practices were possible at the district level. You showed that students benefited from them. You showed that teachers preferred them. I just built on that foundation."

"That's how change works," Maya said. "Someone does the work in one place. Someone else sees it and builds on it. Someone else scales it. Someone else shapes policy around it. You need all the steps. You need all the people. No one person does it alone."

They sat in comfortable silence for a moment, drinking their coffee, looking out at the city.

Maya thought about the trajectory: the Axiom case. The discovery when she first looked at that contract and realized what was happening. The investigation. The prosecution. Garrett Sable in federal prison. Then the slow

work afterward. The district policy development. The state standards writing. The certification program with Delia. The cultural shift in ed-tech. The fact that privacy-first practices were now being considered a competitive advantage instead of a cost or a constraint.

It had taken fifteen years so far. It would probably take another fifteen before the shift was complete. Companies were still collecting more data than they needed. Venture capitalists were still looking for high-growth opportunities in behavioral prediction. The larger system was still fundamentally designed around data extraction as the profit model.

But within that larger system, alternative models had emerged. Alternative ways of thinking about data. Alternative ways of building technology. Alternative ways of contracting and procuring. The baseline conversation was shifting. The questions being asked had changed.

She was no longer the only person working on privacy in education technology. She was one of many. Delia was leading an entire organization. Teachers were demanding better tools and refusing to use tools that felt surveilling. Parents were asking questions about data use. Venture capitalists were taking privacy into account in their investment decisions. School districts were building privacy protection into procurement.

That was how systems actually changed: one person, then two people, then ten, then a hundred, each doing their part, each showing that a different way was possible. Not through revolution or dramatic action, but through steady, patient work, showing that there was a path forward that did not require exploitation.

The Recognition

The invitation arrived in early November, and Maya's immediate instinct was to say no. The American Educational Research Association wanted her to address their annual conference in the spring. The title they proposed was "What Schools Learn from Mistakes: The Axiom Case and System Change." They wanted her to speak for forty-five minutes about what had happened with Axiom and what they had learned from it.

She did not position herself as a researcher or an academic or a public figure. She was a school district employee trying to do her job well. The spotlight made her uncomfortable. Public speaking made her think about things like exit routes and how to control her breathing if she got anxious.

But then she thought about the people who would be in that room. Education administrators. Teachers. Policy makers. University researchers. People who were making decisions about technology in schools. People who were deciding whether to push back against vendor pressure or accept what companies told them was necessary.

If she could speak credibly to what had happened with Axiom, what had gone wrong, what they had learned, how to build systems that were better, maybe that would influence the decisions they made. Maybe it was worth the discomfort.

She called the conference organizers and said yes.

She gave a lot of thought to what to say. The easy version of the talk would be a victory narrative: Axiom was bad, we found the badness, justice was served, the company was punished, the problem was solved. That was the narrative that most people wanted to hear. That was the story that made sense, that had a beginning and middle and end. It was satisfying. It was complete.

But that was not true. The truth was more complicated and less satisfying.

She wrote the talk and practiced it. She sent drafts to Delia and to Jennifer Park and to Tomas, her neighbor and attorney friend who had advised her on the legal issues throughout. She read their feedback and revised. She practiced it out loud so she could feel what the words sounded like when she said them.

The talk she gave was titled "What Schools Learn from Mistakes."

"The mistake is usually obvious after the fact," she began. "You look at what was done and you cannot understand how anyone thought it was acceptable. But you have to understand that at every step, there were reasons. There were incentives. There were institutional pressures pushing toward those decisions. The people involved were not evil. They were operating within a system that pushed them toward bad decisions."

She described the Axiom case from the perspective of someone trying to understand how a company that had intended to build good technology had ended up building a system for exploiting student data. She described the way surveillance had been rationalized as personalization. She described the way profit incentives had shaped every decision. She talked about Garrett Sable not as a villain but as a smart person operating within a system that made bad decisions profitable.

"So the question is not how to fix the individual people," she said. "The question is how to fix the systems. How to create structures and incentives that make it harder to do bad things and easier to do good things. How to build in

oversight so that mistakes are caught early. How to distribute power so that no one person can make unilateral decisions that exploit people."

She talked about the data governance policies that Cascadia had implemented. She talked about the certification program that Delia had created. She talked about the teachers who had reported that privacy-first tools changed how they taught. She talked about students who understood they had agency over their own data.

She talked about the venture capitalists who were beginning to understand that privacy practices were a factor in their investment decisions. She talked about David Hsu and the fact that he was reconsidering his investment strategy because of conversations about aligned incentives.

"This is not about individual virtue," she said. "This is not about finding good people and putting them in positions of power. This is about institutional design. You build systems right and people do the right thing. You build systems wrong and even good people do bad things. The work is not to change individual behavior. The work is to change the systems that shape behavior."

She talked about the slow pace of change. She talked about the frustration of working incrementally when you could imagine revolutionary change. She talked about the value of visible, grounded work even when it did not scale.

The talk was well-received. The conference organizers told her that attendance had been higher than expected, that people had stayed for the Q&A;, that she had received positive feedback. She got email messages from people saying they were inspired by the talk. She got messages from people saying they were going to implement her recommendations. She got messages from people saying they felt less alone in their struggles to protect student privacy.

But she also got critical messages. One person said her analysis was too focused on villain narratives and not focused enough on structural change. Another person said she was naive about market incentives and that privacy-first companies would never compete with exploitative companies. Another person said she was naive about venture capital and that no amount of individual effort would change the system.

Researchers asked for interviews. Universities asked if she would be willing to speak in their programs. Policy organizations asked if she would advise them on privacy frameworks. A foundation asked if she would be on their advisory board. A software company asked if she would consult with them on privacy policy. A nonprofit asked if she would help them develop educational materials about data privacy.

She turned down most of them. But she did agree to meet with a research team at the University of Washington that was studying how schools actually implemented privacy policies. They wanted to understand the gap between policy and practice, between what the policies said and what happened when districts tried to implement them. They wanted to understand why some districts were successful at implementing privacy protections and why other districts struggled. They wanted to understand what the barriers were and what the facilitators were.

The research was honest and rigorous. They found that schools that had strong privacy policies generally had better outcomes: higher teacher satisfaction, better student outcomes, stronger relationships between schools and families. Teachers felt less surveilled and judged by the systems they were using. Students reported feeling more agency over their own learning. Parents reported higher trust in the district. Students were taking more academic risks because they felt safer.

But the policies also required more work, more staff, more administrative burden. They required schools to say no to some opportunities. They required hiring people whose job was explicitly to protect student privacy rather than to maximize data use. They required regular audits and documentation and justification of practices. They required having conversations with vendors about why certain data pipelines could not be used.

"The trade-off is real," Maya said when she reviewed the preliminary findings. "You cannot have strong privacy protection and low administrative cost. You have to choose."

"But schools choose privacy protection when it's framed as protecting children," the lead researcher, a woman named Dr. Sarah Chen, said. "They're

willing to bear the cost when they understand that the cost is the price of ethical practice."

That finding was important. It suggested that the barrier to privacy protection was not primarily economic or technical. It was primarily a matter of will and understanding. Schools would implement it if they decided it was important. Leaders would advocate for it if they understood what was at stake. The question was not whether privacy protection was possible. The question was whether leaders valued it.

"So the work," Maya said, "is changing the conversation. Making it clear that student data is sensitive. Making it clear that protection matters. Making sure that the people making decisions understand what they're choosing when they choose privacy and what they're choosing when they choose data extraction. Making sure they understand the costs, but also understand the benefits."

Dr. Chen was planning to publish the research in several major education journals. She was planning to use it to guide policy recommendations. She was planning to train other researchers to replicate the study in other states. She was creating a movement around evidence-based privacy protection.

"You should be part of that," Dr. Chen said to Maya. "You have credibility that academic researchers don't have. You have the lived experience of implementing these policies. You could help us understand the nuances that the research alone cannot capture."

Maya was tempted. It would be good work. It would generate evidence that would justify the continued expansion of privacy protection in schools. It would create a body of knowledge that future leaders could draw from.

But it would also mean dividing her attention. It would mean spending more time writing about the work and less time doing the work. It would mean becoming an expert commentator on privacy in education instead of a practitioner trying to protect privacy in education.

"I'll help," she said to Dr. Chen. "But I need to keep doing my primary work at Cascadia. I can consult on the research. I can help interpret findings. I can advise on implementation. But I can't step away from the district work."

The research team published their findings in a major education journal. The case study about Cascadia School District became widely read. It was cited in policy papers. It was used to justify funding for privacy initiatives in other districts. Maya became someone people cited when they wanted evidence that privacy-first practices were not just morally superior but actually better for schools.

In the spring, the University of Washington asked her to be the Director of the Center for Educational Data Governance. It was a research and practice position. She would have one foot in academia and one foot in schools. They would hire her at full professor level, with a significant salary increase. She would oversee research, mentor students, consult with districts, give talks, publish papers. She would have resources to fund research. She would have graduate students to work on projects. She would have a platform to speak at national conferences. She would have the credibility of a university position. She would be able to shape curriculum and influence how the next generation of education administrators thought about privacy.

The offer was tempting in ways she had not fully expected. It was not just about money, though the money was significant. It was about influence. It was about being part of an institution that had power to shape thinking and practice across the country. It was about having resources to do research that she had wanted to do but could not find time for. It was about having the validation that comes with a university position.

She sat with the offer for a month. She thought about what she would gain and what she would lose. She thought about the kind of work that actually changed systems versus the kind of work that studied systems. She thought about the distinction between understanding change and making change.

She thought about the years she had spent in Cascadia School District, reviewing contracts, pushing back on vendors, supporting teachers who wanted to do the right thing. She thought about the specific moments that had made her feel like the work was real. The moment she had had lunch with a teacher named Ms. Rodriguez and they had talked about how different it felt to use privacy-first tools. Ms. Rodriguez had said, "With the old software, I felt like I was managing a room full of data points. Now I feel like I'm teaching

students." That conversation had lasted maybe fifteen minutes. But it had been real. It had been rooted in actual practice.

She thought about the time she had sat in a classroom and listened to a seventh grader named Marcus explain that he liked the new system because it didn't make him feel like his mistakes were being recorded forever. She could see the relief on his face. She could feel the safety that he felt in the system. She could understand that she had contributed to that safety.

She thought about the superintendent of Cascadia School District, Patricia Martinez, who had fought for funding to hire Maya even though it was expensive. She thought about the principal who had implemented the privacy-first practices even though they made her job harder. She thought about the teachers who had pushed back on vendors and said, "No, we don't need this data pipeline. No, you cannot track students in this way."

That impact was real. It was visible. It was something she could trace and understand. It was grounded in actual people and actual relationships. If she moved to the university, she would lose that direct connection. She would be able to influence how people thought about privacy. But she would not be able to sit in a classroom and see a student feel safe making mistakes.

She called the hiring director and turned it down.

"I'm not a researcher," she said. "I'm a practitioner. The work I do is grounded in the actual practice of running schools and protecting student data. If I move to a university, I'll lose that grounding. I'll become an advisor instead of a person with power."

"You could do both," the director said. "You could be at the university and maintain your consulting practice."

"No," Maya said. "I can't. I work because I care about the outcome. If I'm not part of the institution making the decisions, I'll lose that motivation. I'll become someone studying the problem instead of someone solving it."

It was the right choice for her. But she recognized that it was also a choice to stay small. It was a choice to not scale in the way that universities offered. It was a choice to keep doing the slow work of changing one institution at a time rather than trying to change the entire landscape through research and

influence.

She was okay with that. She had learned that the most important work was often the least visible work. It was the work of showing up every day to a school district and reviewing contracts and pushing back on vendors and supporting teachers who wanted to do better. It was the work of sitting in classrooms and talking to students about data. It was the work of building relationships with administrators so they understood why privacy mattered.

It was not dramatic work. It did not scale. It did not make her famous or important in the way that university positions offered. But it was work that mattered. It was work that showed up in people's lives. It was work that she could see mattering.

She called the hiring director at the University of Washington and turned down the offer.

"I'm not a researcher," she said. "I'm a practitioner. The work I do is grounded in the actual practice of running schools and protecting student data. If I move to a university, I'll lose that grounding. I'll become an advisor instead of a person with power."

"You could do both," the director said. "You could be at the university and maintain your consulting practice."

"No," Maya said. "I can't. I work because I care about the outcome. If I'm not part of the institution making the decisions, I'll lose that motivation. I'll become someone studying the problem instead of someone solving it."

It was the right choice for her. But she recognized that it was also a choice to stay small. It was a choice to not scale in the way that universities offered. It was a choice to keep doing the slow work of changing one institution at a time rather than trying to change the entire landscape through research and influence.

She was okay with that. She had learned that the most important work was often the least visible work. It was the work of showing up every day to a school district and reviewing contracts and pushing back on vendors and supporting teachers who wanted to do better. It was the work of sitting in classrooms and talking to students about data. It was the work of building

relationships with administrators so they understood why privacy mattered. It was the work of making sure that the policies were not just written but actually implemented, that they were not just announced but actually lived in the daily practice of schools. That work would take her entire career. She was okay with that.

The Perspective

In year nineteen after the Axiom case, something shifted in how Maya thought about what had happened.

She was running on a Friday morning in March, the same route she had run for nearly twenty years, when she realized that she had stopped being angry about what Axiom had done.

Not because she had forgiven them. Not because the violations were acceptable. Not because the harm done to students was unimportant. The anger was gone because she had come to understand something larger: Axiom was not unique. What Axiom had done was what the entire ed-tech industry was set up to do. Axiom had just been more obvious about it.

The systems that exploited student data were not bugs in the educational technology ecosystem. They were features. They were the intended design of the ecosystem. Some companies were more aggressive about exploitation. Some were more subtle. Some masked it better with language about personalization and optimization. Some were genuinely trying to be more ethical. But the exploitation was built into the business model, the business

model was built into the venture capital ecosystem, and the venture capital ecosystem was built into how technology got funded and scaled.

She thought about all the conversations she had had over nineteen years. The venture capitalists who genuinely believed that scale was good. The CEOs who genuinely believed that data was neutral. The politicians who genuinely believed that regulation would stifle innovation. The teachers who genuinely believed that more data meant better instruction. The parents who genuinely believed that companies had their children's interests at heart.

They were all right about some things. They were all operating within systems that made certain beliefs rational and certain decisions profitable. The real question had never been how to punish Axiom. The real question was how to change the industry structure so that exploitation became harder, less profitable, riskier.

That was what she had been working on for nineteen years. Not punishment. Structural change.

She had also come to understand that meeting with Garrett Sable before his sentencing, back when she was still angry and still thought of him as a villain, she had not seen him clearly. He was not a villain. He was a person who had made decisions that had seemed reasonable at the time and that had accumulated into something harmful. He was a person who had operated within a system that incentivized the wrong things.

Garrett believed that he was doing good work. He believed that personalization was valuable. He believed that students benefited from better instruction. He believed that data was the path to better instruction. He believed that sharing data with other organizations was a logical extension of his core business. Each individual decision made sense within the system. The system itself was the problem.

The fact that he was now in federal prison and the venture capital ecosystem was still operating without consequence suggested something was wrong with how they were approaching this problem. They had punished one person. They had not changed the system.

She made a decision on that run. She was going to call Garrett. She was going to tell him something she had learned.

When she got home, she looked up the number for the federal prison where Garrett was incarcerated. She did not know if he would agree to talk to her. But she asked to be put on his call list, and he agreed.

When he picked up the phone, his voice was older than she remembered. He had been in prison for five years now. He had time to think. He had time to understand his decisions. He had time to consider whether his rationalization held up under scrutiny.

"I wanted to tell you something," she said. "I've been thinking about the Axiom case for nineteen years. And I've come to understand something that I didn't understand when you were prosecuted. When I was angry. When I thought of you as the villain."

"What's that?" Garrett asked.

"I don't think you're fundamentally different from the venture capitalists who funded you or the other CEOs who are doing similar things right now," she said. "I think you made decisions that seemed reasonable within a system that was structured to push you toward those decisions. The fact that you're the one in prison and the venture firms are still operating, still funding behavioral profiling companies, still making money, suggests something is wrong with how we're approaching this problem."

There was a long silence on the other end of the phone.

"I appreciate that," Garrett said finally. "But it doesn't make what I did acceptable."

"No," Maya said. "It doesn't. But it suggests that the solution is not to punish individual CEOs. The solution is to change the system. To align the incentives. To make it impossible for the next Axiom to succeed."

"What would that look like?" Garrett asked.

"I don't know yet," Maya said. "But I'm working on it."

After the call, she sat with what she had learned. The Axiom case had felt like a victory when it was happening. The company was exposed. The CEO

was prosecuted and convicted. The contract was suspended. The school district was protected. The students' data was no longer being sold to political micromarketers.

But the underlying structures that had created Axiom had not changed. Other companies were still collecting student data without proper consent. Other venture firms were still funding companies that built behavioral profiling infrastructure. Other school districts were still signing contracts without understanding what they were agreeing to. The industry was still designed to extract maximum data value from every interaction.

The real victory would come when this kind of violation was structurally impossible. When companies could not exploit student data because the systems did not allow for it. When venture capitalists could not profit from behavioral profiling because the regulatory environment had made it unprofitable. When schools had the knowledge and the power to say no.

That was still far in the future. That would require coordination across many institutions. That would require regulation. That would require cultural change. That would require people in positions of power to care about impact, not just about profit.

But it was the work worth doing.

In year twenty, Maya attended a conference for Chief Data Officers in Chicago. There were now over 500 of them across the country, all doing variations of the same work: trying to protect student privacy while still using data to improve schools. The role that she had helped to invent, that had seemed strange and specialized a decade ago, was now becoming standard in districts across the country.

The conference organizers asked her to give the keynote address. The title was "The Long View: Twenty Years of Privacy in Educational Data Systems."

She stood on the stage in the large hotel ballroom and looked out at the crowd of administrators and practitioners who had all taken on this work, who had all decided that protecting student privacy was important enough to make their jobs harder and their work more complicated. There were over 500 Chief Data Officers now, scattered across the country, each of them doing the work in

their own districts.

"The Axiom case happened twenty years ago," she began. "It was a moment that revealed a systemic vulnerability. A moment that showed what could happen when companies prioritized profit over ethics, when school districts were not equipped to understand what they were contracting for, when student data was treated as a commodity rather than as sensitive information about children."

She talked about the specifics of the case. How Axiom had been transparent in some ways, invisible in others. How Project Cornerstone had been a separate pipeline that served different purposes. How Garrett Sable had rationalized the practices by abstracting away from impact. How students' behavioral profiles had been sold to political campaigns, and those profiles had been used to micro-target young voters with psychological manipulation.

"But the case was not just about Axiom," she said. "Axiom was an example of a larger pattern. The venture capital ecosystem funds behavioral prediction. The technology industry builds it. Schools adopt it because they don't understand it. Students are profiled. Data is exploited. And everyone involved tells themselves that their part is benign. The company is just building useful tools. The investors are just funding good technology. The schools are just trying to improve instruction."

She talked about the work that had followed. The policy development. The standards writing. The certification program. The cultural shift. The fact that privacy was now being considered a competitive advantage instead of a cost.

"The work is not done," she said. "It will probably never be done. Because the incentive structures that created Axiom are still in place. Companies still want data. Venture capitalists still want returns. Schools still want tools that work. But each step we take makes it harder for the next Axiom to succeed. Each standard we implement, each certification we create, each teacher who starts to understand that student data is sensitive, each parent who asks questions about data use, makes exploitation harder."

"The work is slow," she continued. "It is frustrating. It is often invisible. Most of you will never know the full impact of what you're doing. You will review contracts. You will push back on vendors. You will support teachers. You will protect student data. And most of the time, nothing dramatic will happen. You will not catch a major exploitation scheme. You will not prevent a landmark case. You will not become famous or important."

She looked across the room. She could see people taking notes. She could see heads nodding. She could see the exhaustion in some faces and the determination in others.

"But you will prevent many small harms. You will make the system incrementally better. And that incremental improvement, across hundreds of districts and thousands of schools, is how systemic change happens. It is not revolutionary. It is not fast. But it is real, and it matters."

After her talk, a Chief Data Officer from a district in Texas approached her. She was probably in her forties, with the tired but determined expression of someone who understood what was at stake and was committed to the work anyway. Her name was Rebecca Torres, and she ran the data governance program for a district serving 50,000 students. She had gray in her hair and permanent lines around her eyes from years of navigating complicated institutional politics.

"How do you keep doing this?" Rebecca asked. They were sitting in a quiet corner of the conference hotel, away from the crowds. "How do you keep caring about it after twenty years?"

"I keep seeing the impact," Maya said. "I keep talking to teachers who say their work is better. I keep talking to students who understand they have agency over their own data. I keep seeing that the work matters."

"But doesn't it get exhausting?" Rebecca asked. Her voice had an edge to it, something like desperation or fatigue. "Knowing that no matter how much you do, there's always more? Knowing that the venture capitalists are still out there, still funding companies, still trying to extract more data? Knowing that the system is still designed to exploit?"

"Yes," Maya said. "It does. But that's true of all important work. You don't finish. You just keep going. You do your part. You help other people understand what's at stake. You create conditions where other people can do their part. And somehow, over time, the system shifts."

Rebecca was quiet for a moment. She was looking at her hands, which she had folded on the table.

"I implemented the state standards in my district," Rebecca said. "I trained my whole team. We built new processes. We hired a new person just to manage data governance. We said no to several vendors that wanted to collect more data than we were willing to allow. Our teachers are happier. Our families report more trust. By every measure, it's working."

"That's good," Maya said.

"But every quarter, I get pressure from my superintendent about budget," Rebecca continued. "He's asking whether we could implement cheaper tools if we relaxed some of the privacy policies. He's asking whether we could generate more data to improve instruction. He's asking whether we're being too restrictive. The pressure never ends. The moment you stop pushing back, you start sliding backward."

"That's the work," Maya said. "That constant vigilance. That constant pushing back. It never stops."

"How do you sustain that?" Rebecca asked. "How do you not burn out? How do you not just give up and say, 'Fine, collect all the data, use it however you want, I'm done fighting'?"

Maya thought about the question. It was a real question. She had asked it herself many times. The work was never done. The victory was never complete. The system was always trying to reassert itself.

"I sustain it by remembering why I started," Maya said. "I sustain it by remembering the feeling of discovering what Axiom was doing. The feeling of understanding that a company was building behavioral profiles of 38,000 students and selling them to political campaigns. That children's personalities and vulnerabilities were being packaged as products. That someone, somewhere, was using this data to manipulate young voters."

"That makes me angry," Rebecca said.

"Yes," Maya said. "That anger is sustaining fuel. But you can't run on anger alone. It burns you out. So alongside the anger, I keep the hope. I keep the belief that a different way is possible. I keep the evidence that it's working. The teachers who feel less surveilled. The students who feel more agency. The parents who trust the schools more."

"But what if it doesn't work?" Rebecca asked. "What if we do all this work and the system doesn't shift? What if in ten years, a new Axiom emerges? What if we're just rearranging deck chairs while the ship sinks?"

"Then we will have made life better for the students and teachers in our districts," Maya said. "That matters. It counts. It is not nothing."

"But it feels like nothing when you're fighting against an entire industry designed to exploit," Rebecca said. "It feels like we're working for crumbs while the venture capitalists are making billions."

"I know," Maya said. "I feel it too. I feel it every day. The frustration that the system is still fundamentally misaligned. The anger that one person is in prison for doing what the entire industry does. The despair when I look at what's still possible in behavioral prediction. The fact that we've fought so hard and we've only achieved incremental progress."

She paused.

"But here's what I've learned: incremental progress compounds. A few districts implement privacy protections. Then other districts see it works and they do it. Then teachers prefer working in districts with privacy protections. Then families prefer schools with privacy protections. Then vendors start to see that privacy is a competitive advantage. Then investment starts flowing toward privacy-first companies. Slowly, over time, the baseline shifts. It's not revolutionary. It's not fast. But it's real."

"And what if the baseline doesn't shift?" Rebecca asked. "What if we've spent years of our lives on this and it doesn't actually change anything?"

"Then we tried," Maya said. "We stood against a system designed to exploit children. We pushed back against people who wanted to extract more and more data. We created space for teachers and students to work without

feeling surveilled. We did the work that our conscience told us was right. That matters."

Rebecca was quiet for a long time. They sat together in the conference hotel lobby, watching people walk past, most of them tired from the conference, most of them worried about the work waiting for them in their districts.

"I'm going to keep doing it," Rebecca said finally. "I'm going to keep implementing privacy protections even though it's hard and the pressure is constant and I never know if it's actually working."

"Because?" Maya asked.

"Because last year, a student came to me in my office," Rebecca said. "She was in high school, seventeen years old. She said that she appreciated that our district had privacy protections because she wanted to be able to make mistakes without having them recorded forever. She said that she had friends in other districts whose schools used heavy data monitoring, and those friends were afraid to take risks academically because they knew the system was watching every move. She said that feeling watched made her anxious and made learning harder."

Rebecca's voice got quieter.

"She said that because our district protected her privacy, she could focus on learning instead of on being evaluated. She could try hard things without fear that her struggles would be permanently documented. She could be a student instead of being a data point."

"That's why," Maya said.

"That's why," Rebecca echoed. "That one conversation was worth all the pushback, all the budget meetings, all the frustration. One seventeen-year-old understanding that her privacy mattered. One student feeling safe enough to learn."

"That's the work," Maya said. "That's what it's for."

Rebecca looked at Maya directly for the first time since they started talking. "Are you going to keep doing this for another twenty years?" she asked.

"I don't know," Maya said. "Maybe. Probably. Until I can't. Until I'm too tired or the work has changed so much that I don't recognize it anymore. But yes, I think for at least another twenty years."

"I envy that," Rebecca said. "That certainty that you know what you're supposed to be doing."

"I don't know that I have certainty," Maya said. "I have commitment. I have clarity about the values that matter to me. I have evidence that the work matters. But I don't have certainty that we're going to win. I don't have certainty that the system is going to change. I just have a decision that this is the work worth doing, so I'm going to do it."

They sat in silence for a few more minutes. Around them, the conference continued. People were networking, exchanging contact information, talking about implementation strategies, sharing horror stories about vendors who refused to respect privacy policies. The movement was real. The work was happening. One district at a time, one teacher at a time, one student at a time, people were choosing to protect privacy instead of just collecting data.

That night, in her hotel room, Maya thought about what twenty years looked like. She thought about the person she had been when she had first met Priscilla Holt at the Axiom offices, not yet understanding what she was looking at. A person who knew something was wrong but didn't yet know how to articulate it. A person who was still learning to trust her instinct that data collection could be a form of surveillance even when people called it personalization.

She thought about the months of investigation that followed. The slow accumulation of evidence. The moment when Project Cornerstone became visible. The understanding that Axiom had explicitly designed a second data pipeline to enable behavioral profiling and political targeting. She thought about the prosecution. The conviction of Garrett Sable. The fact that one CEO went to prison while the venture capital ecosystem continued operating.

She thought about the years of work afterward that nobody would ever see in a documentary or read about in a news article. The mundane work of contract review. The frustrating conversations with vendors. The slow building

of standards. The endless education of people who did not understand that data collection was a choice, not an inevitability.

She thought about the timeline in her head: the contract audit, the discovery of Project Cornerstone, the investigation, the prosecution, Garrett Sable's conviction, the initial policy work at Cascadia, the state standards development, the certification program with Delia, the expansion to other districts, the research that proved privacy-first practices actually worked better, the recognition in the field, the conversations with venture capitalists, the shift in the baseline expectations about what was acceptable.

It was a good timeline. It was a timeline of actual change. It was also a timeline of incremental progress, not revolutionary transformation. The changes had not happened overnight. They had not happened because anyone had willed them into existence. They had happened because enough people, in enough places, had decided that protecting students mattered more than collecting data.

The larger structures were still in place. The venture capital industry was still designed around scale and growth and extraction. Companies were still looking for competitive advantage through data. The incentive structures were still misaligned in many ways. Companies still made decisions based on profit, not ethics, though profit and ethics were sometimes starting to align. But within those larger structures, alternative models had emerged. Alternative ways of thinking about data. Alternative ways of building technology. Alternative ways of contracting and procuring.

She did not know if those alternatives would eventually dominate. Probably not entirely. Probably the landscape would always be mixed, some companies exploiting, some companies trying to protect privacy, most companies somewhere in the middle, trying to balance profit with responsibility.

But she knew the alternatives existed now. And she knew they mattered. And she knew that the existence of alternatives meant that people had choices.

She thought about the teacher in the classroom who had said the new system helped him focus on students instead of managing data. Marcus, or

maybe someone like Marcus. She thought about the student who had said she felt less like she was being spied on. That student was probably in high school now, probably did not think much about her school's privacy practices, probably took it for granted that her data was protected. But she was doing better in school because she was not afraid of making mistakes. She was learning in a way that felt safe.

She thought about the principals who had reported higher job satisfaction when they used privacy-first tools. She thought about the school districts that had adopted strong governance standards because they understood that protecting student privacy was the right thing to do. She thought about Cascadia School District, where it had all started. The district was still implementing these practices. Teachers were still asking privacy questions. Families were still being asked for genuine consent instead of being presented with pre-filled forms.

That was change. Not revolutionary, but real. And real was what mattered.

She opened her laptop and started drafting notes for next year's work. There were districts that needed support implementing standards. There were companies that needed to be pushed toward more ethical practices. There was research that needed to be done to understand what worked and what didn't. There was a system that needed to be changed, one institution at a time, one decision at a time, one conversation at a time.

She thought about calling Garrett Sable again. She thought about what she would tell him if she did. That his conviction had meant something, but not everything. That changing the system was harder than punishing one person. That the real work was showing that alternatives were possible.

She thought about David Hsu and the venture capitalists who were reconsidering their investment strategies. She thought about the fact that money was slowly beginning to flow toward companies that prioritized privacy. She thought about the fact that transparency was becoming a selling point instead of a liability.

She thought about Delia and her nonprofit, growing in scope and impact. She thought about the fact that they had created an entire framework that was

being adopted across the country. She thought about the fact that other states were now writing privacy standards based on the Washington State model. She thought about the fact that countries were asking about this work.

Outside her window, Chicago stretched out into the dark. The city was full of schools. Thousands of them. Millions of students. Each one of them with data being collected, decisions being made based on that data. Most of it probably good data, used for good purposes. Some of it probably bad data, used to exploit or control.

Twenty years of work had not solved the problem. But it had moved it. It had made it harder to exploit. It had created enough evidence that a different approach was possible that other people were choosing to build differently. It had shown that teachers preferred working without feeling surveilled. It had shown that students learned better when they felt safe. It had shown that schools could make decisions based on values instead of just on what was profitable.

That was enough. It had to be enough. And somehow, after twenty years, looking out at a city full of people working in schools, working with students, trying to do right by them despite the systems that pushed against them, it felt like it actually was.

She sent her notes to Delia and to Jennifer Park and to Tomas. She sent a message to Daniel saying hello and asking how his company was doing. She made a note to visit Cascadia District next month and sit in on some classrooms and talk to teachers about how they were managing the work.

Then she went to sleep, and she dreamed about classrooms where students felt safe making mistakes, where teachers felt trusted to teach, where data was a tool instead of a weapon. It was not a vision of the future so much as a vision of what was possible. And the fact that it was possible, that it existed in some places and could exist in more places, was enough to keep going.

The Choice

In year twenty-one, Maya was offered the position of deputy superintendent for the Cascadia School District. It was a promotion. It was a significant jump in responsibility. It meant moving from being Chief Data Officer to being part of the senior leadership team, responsible for curriculum and instruction and operations. It was also a move that would take her further from the actual work of protecting student data. She would be managing managers. She would be in more meetings and fewer conversations with teachers.

She sat with the offer for a week, turning it over in her mind the way she turned over anomalies in data: looking for the pattern, the thing that didn't fit. The superintendency would be power. It would be influence. It would be the kind of promotion that people spent their careers chasing. And it would remove her from the thing that actually mattered, which was the protection of student data at the ground level, where the real work happened.

She thought about what it would mean to accept it. She would move into a corner office on the third floor. She would attend cabinet meetings every Monday morning. She would oversee budget allocations across the entire

district, managing millions of dollars, managing principals, managing the dozens of other administrators who made the system run. She would be further from teachers, further from the actual technology, further from the moment-by-moment decisions that determined whether data was protected or extracted. She would spend her days in meetings about budget negotiations and board relations and the political management of a public institution. She would spend her nights at events, smiling at school board members, performing a role.

She thought about what it would mean to decline. She would stay in her role. She would continue the work she was good at. She would continue to understand what was happening to student data, who was collecting it, how it was being used, whether that use was appropriate. She would continue to be the person who could see the threat coming and could say no. She would continue to be in the room when vendors pitched their systems. She would continue to understand the technical details that mattered. She would continue to protect. But she would also watch other people climb the ladder while she remained in place. She would hear, over the years, that she had peaked, that she chose safety over ambition, that she had settled.

The promotion felt like a test. Not of her competence, but of what she actually valued. What she actually wanted. Whether she wanted the appearance of power or the actual ability to protect.

In the end, she went to talk to Priscilla Holt, who was retired and living in Seattle and whom she had stayed in contact with over the years. They met at a coffee shop near the water, a place where nobody was paying attention to anyone else, where conversations could be real instead of performed. Priscilla was smaller than Maya remembered, the way people become smaller when they are no longer in power. Age had reduced her. Time had softened her.

"They offered me deputy superintendent," Maya said, stirring coffee she wasn't going to drink.

"Are you going to take it?" Priscilla asked.

"I don't know," Maya said. "It's a good opportunity. But I'm worried about losing the thing I care about, which is the actual work."

Priscilla was quiet for a long moment. She was the kind of person who didn't fill silence with noise. She let silence sit. She let it mean something. "You will," she said finally. "If you take that job, you will have less time to do the actual work of protecting student data. You will spend more time in strategy and politics and budgeting. You will spend more time managing perception and fighting for resources and navigating the egos of people who are threatened by your competence. You will spend less time actually understanding what's happening with student information."

"So you think I should decline," Maya said.

"I think you should do what's right for you," Priscilla said. "But I'll tell you what I learned as superintendent. The higher up you go, the further you get from the actual work. At some point, you're no longer solving problems. You're managing the people who solve problems. You're managing the people who manage the people who solve problems. And by the time you get there, you've forgotten what the actual problems look like. You've forgotten what the actual consequences of your decisions are because the consequences are so far removed from you."

"I like solving problems," Maya said.

"I know you do," Priscilla said. "That's why you're good at what you do. You're good at it because you understand the details. You understand the technical side. You understand what the data means. You understand what the threats are. You understand what it takes to protect against them. I would suggest staying in the role you have. You've built something good there. You've built something that works. You've created systems where student data is protected not because someone is constantly fighting for it, but because protection is built into how the institution operates. That's rare. That takes years to build. If you move up, you'll be managing other people to do what you're good at, and you might not be good at managing other people. More importantly, you'll stop understanding the actual technical and practical work. And then when you try to lead people who do that work, you'll be leading blind."

"I could be good at managing," Maya said. "I could learn."

"You could be," Priscilla agreed. "But why learn a new skill when you're already excellent at what you're doing? Why stop doing what matters to learn to manage people doing what matters? The world doesn't need another administrator. The world needs more people who actually understand how to protect student privacy at scale. Who understand the details. Who understand the threat. Who can say no to vendors because they understand what the threat is."

They sat with that for a while. A ferry passed in the distance, moving from one pier to another, steady and reliable. It was the same ferry route that had been running for thirty years. It moved slowly, but it moved reliably, and it got people where they needed to go. Maya had always thought that was a decent metaphor for institutional work. You moved slowly, but you moved in the right direction, and you got people where they needed to be.

It was a simple argument and probably the right one. Maya declined the deputy superintendent position that evening, by phone, with three words: "I'm going to decline."

The superintendent called her into his office the next day. He was a good man, but he operated at the level of systems and politics, not details. That was his job. That was what he was good at. It was also what prevented him from understanding why she would decline a promotion. Power in his world looked like hierarchy. In her world, it looked like the ability to actually protect.

"Why?" he asked, genuine confusion on his face.

"I'm more effective in my current role," she said. "I understand how to protect student data. I understand the technical and governance side. I understand how to push back on vendors and support teachers. I understand what questions to ask and what the answers mean. I understand what I'm looking for when I review a contract. If I move up, I'll be learning a new role and I'll be less effective at both. And student data protection will go down the priority list because it's not something the administration understands deeply. It's not something the superintendent thinks about. So it will be whatever priority gets assigned to it, and it will be lower than it should be."

"You're sure?" the superintendent asked. "This isn't about money. We can talk about money."

"Yes," Maya said. "I'm sure."

She did not know if declining the promotion was the right choice or just the choice she preferred. But she knew herself well enough to understand that advancement through organizational hierarchy was not what motivated her. Impact motivated her. The ability to actually protect student data motivated her. The ability to see the result of her work motivated her. The ability to sit in a classroom and know that a teacher had better information about student learning because she had shaped how that information was collected and protected. The ability to say no to a vendor because she understood what the threat was.

A promotion would cost her those things. A promotion would change her from someone who understood the work to someone who managed other people to do the work. And she had seen enough of that kind of transition to know that it rarely worked well. Once you moved away from the actual work, you lost the credibility to manage the people doing it. You lost the knowledge to guide them. You lost the ability to see when they were making mistakes.

She was fifty-five years old. She had been doing this work for twenty years. She had not planned to stay at Cascadia School District forever. But as she looked at what else she might do, nothing seemed as meaningful as what she was already doing. She could retire. She had enough savings. She could travel. She could write about her experience. She could advise other districts without being employed by one. She could become a consultant, moving from district to district, solving their data problems, and moving on.

But all of those alternatives would have meant stepping back from the actual work. And stepping back felt wrong. It felt like abandoning something that mattered. It felt like choosing comfort over responsibility. It felt like forgetting what she had seen and what it meant.

She went to talk to Tomás, who had become her closest friend over the twenty years of knowing him. They had met at MPSA, both as students, both young and angry about systems that didn't work. They had stayed friends

through his career in intelligence and her career in data security. He was one of the few people who understood the work because he had done parallel work in a different field. He had stayed in the work instead of moving up. He understood the choice.

They ran together at five AM, the way they did twice a week, the way they had done for the last decade. Running in silence. Moving through the city before it woke. Just the rhythm of their feet on the pavement and their breath and the darkness.

"I turned down a promotion," she said. They were crossing the bridge over the canal, the city still quiet below them.

"Why?" he asked, not breaking stride.

"Because I would be less effective in the new role," she said. "Because I would stop doing the actual work and start managing other people doing the actual work. Because I would become the thing I don't want to be."

"That's the best reason to turn down a promotion," Tomás said. "Most people turn down promotions for dumb reasons. Ego. Fear. Territoriality. Some weird commitment to status that they don't even understand. You're turning down a promotion because you've thought carefully about what you're good at and what matters to you."

"I'm going to be doing the same job for another decade," Maya said. "Maybe longer. That seems limiting."

"Or it seems focused," Tomás said. "You found something that matters. You got good at it. You're staying with it. That's not limiting. That's commitment. That's the opposite of limiting. That's one of the few things that actually means something."

They ran in silence for a while, their feet hitting the pavement in the darkness. The city was quiet at this hour. There were other runners, other people who had chosen to be awake before the world started moving. There were other people who understood that some mornings were better than others, that some moments mattered, that you had to protect the things that mattered or they would be taken from you.

"I'm worried I'm making a mistake," Maya said.

"You would make a bigger mistake taking the job," Tomás said. "You would spend the next ten years managing meetings and budgets and politics. You would lose the thing that makes you who you are. You would lose the ability to actually understand what's happening to student data. You would lose the ability to protect. And then you would retire and realize you spent the decade of your sixties becoming something you didn't want to be. That would be a mistake."

"It's not ambitious," Maya said.

"Ambition is not a virtue," Tomás said. "Doing something well is. You're doing something well. Excellence is worth more than ambition. That's a truth they don't teach you in school. They teach you to be ambitious. They teach you to climb the ladder. They don't teach you that climbing the ladder is often a trap. That the actual work is down here, not up there. That excellence matters more than hierarchy. Stay with that."

So she stayed. She continued to review contracts. She continued to push back on vendors. She continued to support teachers. She continued to see the actual impact of the work. She continued to be the person who understood what was happening to student data and who fought, every day, to keep that data from being exploited. She continued to be in the room when vendors pitched their systems. She continued to be the person who could ask the right questions and understand the answers.

The Axiom case had happened twenty years ago. It had exposed a vulnerability in how schools handled data. It had led to policy changes. It had led to industry changes. It had led to a whole field emerging around protecting student privacy in educational technology. It had changed her life, though she had not known it at the time.

But the underlying vulnerabilities remained. New companies were building new systems designed to exploit student data. New venture firms were funding the exploitation. New justifications were being offered for why data collection and use were beneficial. New technology made data collection easier and more invisible. New algorithms made it possible to extract value from data in ways that had not been possible before. The threat did not end. It evolved.

The work would never be finished. The threat would always be present. But the defenses were also getting stronger, and she was part of building those defenses. Every contract she negotiated. Every vendor she pushed back on. Every policy she helped create. Every teacher she educated about what data they actually needed. Every student whose data was protected because the systems were designed to protect it.

Maya had chosen to stay on the front lines of that work. Not as a policy maker. Not as a researcher. Not as a venture investor trying to change incentives. But as a person actually running a school district and making decisions about what data was collected and what was done with it. She was the person in the room when vendors pitched their systems. She was the person who asked the hard questions. She was the person who said no when she needed to say no.

It was not glamorous work. It was not work that would make her famous. It was not work that would lead to a book deal or a TED talk. But it was work that mattered. And as she looked back over twenty years of doing it, she could see that mattering was enough. Mattering was everything. Mattering was the only reason to stay in one place and keep pushing, keep fighting, keep protecting.

She had made her choice. She would stay. She would fight. She would protect. She would understand the details and maintain the ability to see the threat. She would be the person in the room who understood.

That night, after her decision was final, she sat in her apartment with a cup of tea that she wasn't going to drink and thought about the twenty years she had already invested. She thought about Axiom. She thought about the years of building systems and policies. She thought about the teachers she had supported and the students who had been protected because she had said no at the right moment.

She thought about the people who had left the field. She thought about the consultants who had moved on to bigger firms. She thought about the advocates who had burned out from the constant fighting. She thought about the researchers who had gone into academia where the work was more

theoretical. She had stayed. She would keep staying.

The decision felt right in a way that the promotion had not felt right. The promotion would have been easier. The promotion would have looked good on a resume. The promotion would have been the thing that people would point to as success. But it would have been someone else's definition of success. It would not have been her definition.

Her definition of success was that student data in her district was protected. That teachers understood what data they actually needed. That vendors understood that they couldn't extract unlimited amounts of information. That students knew what was happening to their data. That privacy was normal. That privacy was expected. That you had to justify extraction, not protection.

That was what success looked like. And she could see that success every day if she stayed. She could see it in the contracts that she had negotiated. She could see it in the policies that had been implemented. She could see it in the students who were protected. She could see it in the teachers who had learned to think carefully about what data they asked for.

She had made her choice. She would see it through.

The New Problem

In year twenty-two, a new category of education technology began to emerge: AI-based tutoring systems. These systems claimed to be even more personalized than previous technologies, even more responsive to individual student needs. They also required even more data. The systems needed constant feedback on how students were learning in real time. They needed to understand not just what students knew, but how students thought, what they understood intuitively, where their misconceptions came from. They needed to build models of each student's learning process so detailed that they could be used for purposes beyond teaching: prediction, profiling, behavioral modification. They needed to extract.

Maya saw it coming. She had been in the industry long enough to recognize the pattern. She could see the threat the way a chess player could see three moves ahead. New technology emerged that was genuinely useful for teaching. She approved it with modifications. Teachers used it. Students benefited. The educational benefit was real. And then the company started expanding what they did with the data. Retention periods lengthened. New uses emerged. Profiles were built. The educational tool became a data extraction

tool. The cover story gave way to the actual business model.

The first company to approach Cascadia with an AI tutoring system was called Luminance Learning. They had a compelling pitch, the kind of pitch that appeared in venture funding documents and on conference panels and in the minds of people who dreamed about transforming education through technology. Their system could identify exactly what a student misunderstood and could adjust instruction in real time to address the misunderstanding. Students could move at their own pace. Teachers could focus on the students who were struggling most. Teachers could have more time for actual teaching instead of grading. It was a vision of personalized learning that had been promised for thirty years. It was also, from a data governance perspective, a nightmare.

Maya scheduled the meeting for her office on a Thursday afternoon. She prepared by reviewing Luminance's public materials, understanding what they were going to pitch, understanding what the real threat was. She prepared by asking herself what questions would reveal the infrastructure beneath the pitch. She prepared by reminding herself that the pitch was not the product. The pitch was the cover story.

"How much data does this require?" Maya asked in the initial meeting with Luminance's representatives. She sat across from them in her office, her computer off, her attention entirely on their faces and their answers. This was her skill: listening not just to what was said, but to what was implied by how it was said, to what was being avoided, to where the discomfort lived. She could read the data in human behavior the way other people read documents.

"Comprehensive learning data," they said. "We need to understand what students get right and wrong at a granular level. We need to understand their problem-solving processes. We need to understand their learning patterns. The more granular the data, the better the system performs."

That was the answer she expected. That was always the answer. More data meant better algorithms. Better algorithms meant better product. Better product meant more customers. More customers meant more data. It was a beautiful feedback loop for the company and a nightmare for privacy.

"How long do you retain that data?" Maya asked.

"For the duration of the contract," they said. "It allows us to continuously improve the algorithm."

"And after the contract ends?" Maya asked.

"We can delete it," they said. But they hesitated. They glanced at each other. There was discomfort. "But the data is valuable for algorithm improvement, so we ask if the district would be willing to allow us to retain it for research purposes."

Translation: We want to keep the data. We want to keep using it. We want to keep extracting value from it. And we want your permission to do that. And we're banking on you not understanding what we're asking for.

"Who has access to the data?" Maya asked.

"Our engineers and data scientists," they said. "And potentially our research partners at universities."

"Do you run any secondary processing on the data?" Maya asked. "Do you build profiles? Do you sell the data? Do you use it to train models that you then sell?"

"We do not sell the data," they said. But there was something in that response. Something in the way they said it. Not selling data was technically accurate. What they were doing was using data to train models that they sold. They were using data to extract value. They just weren't selling the raw data.

"But we do use it for research and for algorithm improvement. We also build profiles internally to understand learning patterns."

Maya made notes. She listened. She asked questions about what the profiles looked like, who could access them, how long they were retained, whether they could be matched against other data sources. With each answer, the picture became clearer. This was not a tutoring system. This was a behavioral profiling system that happened to have a tutoring interface. The teaching was the cover. The data extraction was the goal. The company had figured out how to make a tool that was actually useful for education and then use that usefulness as a cover for extraction.

"Show me the system," Maya said.

They showed her the interface. She sat at the computer and clicked through the interface, understanding what it was designed to do. It was beautiful. It was intuitive. It showed exactly what students had gotten right and wrong. It showed learning trajectories over time. It showed where students were struggling. It showed predictions about what would cause them to struggle next. As a teaching tool, it was excellent. As a data governance system, it was a disaster waiting to happen. The system captured not just what students knew, but how they thought, where they had anxiety, what their learning patterns revealed about their cognitive strengths and weaknesses. All of that could be used to predict behavior, to identify students at risk, to categorize students by ability. All of that could be weaponized.

"I'm not approving this," Maya said. "Not in this form."

"Why not?" the Luminance representatives asked, clearly surprised. They had been confident in their pitch. They had been confident that the educational benefit would be obvious. They had been confident that she would say yes.

"Because you're asking me to allow you to collect comprehensive learning data on every student, retain it indefinitely, and use it for purposes beyond teaching," Maya said. "Because your contract does not specify what happens to the profiles you build. Because you're asking me to trust that you won't do with the data what other companies have done with similar data. Because I've seen what happens when companies get access to comprehensive data on students. I've seen what the threats are. And I'm not going to gamble with student privacy."

"But the system is designed to help students," they said.

"I don't doubt it," Maya said. "But the system is also designed to extract value from student data. You're combining an educational tool with a data extraction system. I'm not going to sign the contract."

They left, clearly frustrated. They had expected the yes to be easier. They went to the superintendent's office. They made their case to him. He called Maya into his office an hour later.

"Why can't we use this system?" he asked. "It sounds like it could really help students. The teachers are asking about it."

"Because the contract is not acceptable from a privacy perspective," Maya said. "Because the system is designed to extract and retain data in ways that we've said we won't allow. I've explained this in my written recommendation. I can walk you through the specific concerns if you want."

"But students might benefit," he said.

"They might," Maya said. "Or they might be harmed by having their every learning move tracked and analyzed and retained and used to build profiles. The benefit is speculative. The harm is clear. The data extraction is certain. This is a choice we have to make deliberately. Are we going to prioritize the educational benefit or the privacy protection? If we choose educational benefit, we accept data extraction. If we choose privacy protection, we might miss some pedagogical advances. I'm recommending we choose privacy protection."

"What if we negotiate better contract terms?" he asked.

"I'll review them," Maya said. "But I want to be clear about what I'm seeing here. This is a company that has built a tool that is useful for teaching. They're now trying to expand how much data they can extract from students using the promise that the tool will help them. This is how it always works. The education is the cover. The data is the value. This is the pattern that I've seen repeat itself for twenty years."

Luminance came back with a revised contract. They had listened. They understood that Maya was not going to approve the original contract. They came back with modifications. They agreed to limit data retention to the duration of the contract plus one year. They agreed to delete comprehensive learning records after that period and retain only aggregated data that could not be matched to individual students. They agreed to not build individual student profiles without explicit parental consent. They agreed to not share data with third parties without district authorization.

It was better. It was still not ideal from a privacy perspective. The system would still collect enormous amounts of data. The teaching interface would still serve as a data collection mechanism. The profiles would still be built, at least

temporarily. But the retention period was limited. The secondary uses were constrained. The district maintained control over the data.

"I'll recommend we approve this," Maya said. "But I want to flag that this represents a new category of risk. These systems are getting better at tracking student learning in real time. That's good for instruction. It's also good for behavioral profiling. It's good for building models of how students think. It's good for identifying vulnerabilities and exploiting them. We need to be careful about which of these companies we allow into our schools."

The district approved the revised contract with Luminance. They implemented the system in three schools as a pilot. Maya insisted on being part of the evaluation team so she could monitor what was actually happening with student data. This was not a check that could be delegated. This was something she needed to understand directly.

She sat in classrooms where the Luminance system was being used. She watched students interact with the system. She watched them type, watched them solve problems, watched them experience the feedback the system was providing. She talked to students about their experience. She asked them if they understood that the system was collecting data on their learning. Some did. Some didn't. Some thought the system was just helping them learn and didn't think about what the data was being used for. That was the problem. The students didn't see the data extraction because the educational benefit was real. The system was helping them. So the data collection felt invisible.

She reviewed the data that was being collected. She looked at the technical documentation. She tracked what was being done with the data. She looked for secondary uses, for profile building, for retention beyond what the contract specified. She was looking for violations. She was looking for drift. She was looking for the moment when the company started pushing on the boundaries that had been set.

It was better than she had feared and worse than she had hoped. The system was genuinely useful for teaching. Teachers could see exactly where students were struggling. They could adjust their instruction based on real-time feedback. Student engagement improved. Student learning improved. The

educational benefit was real. She could see it. She could see the teachers using the data to make better decisions. She could see the students learning better. The system was working.

But the data collection was more comprehensive than she would have preferred. The system captured learning patterns that were revealing. It captured not just what students knew but how they thought. Even with the contract restrictions, there were gaps in oversight. The system was managed by company engineers who were thousands of miles away. The district had visibility into what data was collected, but less visibility into what was done with it once it left the district's systems. There was risk. There was always risk.

More importantly, she could see how the system could be modified to become extractive rather than educational. All of the infrastructure was there. All that would need to change was the incentive structure. A change in company ownership. A change in business model. A change in what counted as success. And the system would transform from a tool for teaching to a tool for behavioral profiling. The possibility was built in.

"This is the future," she told Delia Park in a call about updating the privacy-first certification program. Delia had left Axiom years ago and had become the director of the privacy-first certification project, something they had dreamed about together years before. Delia was doing work that mattered. She was building standards. She was changing the industry. She was making the future better. "These systems that are designed to help students are also designed to extract data. The question is whether we can create an industry norm where that data extraction is constrained."

"Can we?" Delia asked. She sounded tired. She was building standards that companies resisted. She was fighting the same battles Maya was fighting. She was pushing back on the incentives that rewarded extraction. It was exhausting work.

"We might be able to," Maya said. "But we need to be intentional about it. We need to require transparency. We need to require that schools know what data is being collected and what it's being used for. We need to create accountability. We need to make sure that the educational purpose is primary

and the data extraction is secondary, not the other way around."

Over the next year, Maya and Delia updated the privacy-first certification standards to include specific requirements for AI-based learning systems. Companies had to demonstrate that their algorithms could work with limited data. They had to show that they were not building profiles. They had to allow for data deletion. They had to limit retention periods. They had to provide transparency into what data was collected and how it was used.

Luminance applied for certification. They had to make significant modifications to their system to meet the standards. It was hard. It required engineering work. It required rethinking how they built their algorithms. It required sacrificing some of the things that made their system powerful. But they were willing to do it. By year twenty-four, they were the first AI tutoring system to be privacy-first certified. It was a different model than the traditional surveillance-based approach that other AI tutoring companies were taking. It was less effective at tracking every moment of learning. But it was more ethical and students knew what was happening with their data.

Maya took satisfaction in the fact that you could have good technology and ethical practices. They were not incompatible. It just required being intentional about which you prioritized. It required saying no to companies. It required pushing back on the seduction of better teaching through more data extraction. It required building alternative models where teaching could be good without being extractive. It required work.

As she looked at the next generation of educational technology challenges, she realized that the work would never truly be finished. There would always be new technologies that promised to revolutionize learning and that created new opportunities for data extraction. There would always be new incentives pushing toward exploitation. There would always be new vulnerabilities to identify and close. There would always be companies that saw students as data sources instead of people.

But there would also be people who understood this. There would be people who would say no. There would be advocates and researchers and teachers and administrators who would push back. There would be companies

that would choose to build better systems. There would be parents who would ask questions. There would be students who would understand, as Zara did, that something was wrong, and who would do something about it.

The Luminance case was just the beginning. There would be other systems. There would be other vendors. There would be other moments when she would have to decide whether to approve a contract or push back, whether to accept what was offered or demand something better. There would be years and years of that work ahead of her.

But she understood now that this work was not burden. It was purpose. It was the thing she was good at. It was the thing that mattered. And as long as she could do it, she would do it. She would keep reviewing contracts. She would keep asking hard questions. She would keep saying no to systems that extracted too much and demanded too little accountability. She would keep building a school district where student privacy was not an afterthought but a fundamental commitment.

This was her work. This was what she did. This was what she would continue to do for as long as she could.

The Ecosystem

By year twenty-four, Maya had built a network. It was not a formal network. It was not an organization with membership or dues. But it was a network nonetheless: the people working on privacy in education across the country. There were the Chief Data Officers in the five hundred districts that had hired people like her. There were the researchers studying privacy in schools, publishing papers that questioned the assumptions underlying data collection, showing evidence that surveillance did not actually improve learning. There were the advocates pushing for privacy regulation, fighting for laws that would protect student data. There were the companies building privacy-first technology, understanding that there was a market for ethics. There were the lawyers developing policies and standards, creating the legal frameworks that made protection possible. There were the teachers who understood that data collection had to serve students, not extract from them.

They did not all know each other. They did not all agree with each other on everything. But they were all, in their own ways, working to constrain the extraction of data from children and to protect student privacy. They were all pushing against the same incentive structures that rewarded data extraction and

penalized privacy protection. They were all trying to build institutions that could be trusted with student information. They were all fighting the same fight, even if they didn't all know each other's names.

The network worked because the problem was large enough and urgent enough that there was room for different approaches. Some people worked at scale, building standards that could be adopted across the country. Some people worked at the local level, managing the data in individual districts, fighting the battles in individual classrooms and schools. Some people worked in regulation, pushing governments to create laws that protected privacy. Some people worked in technology, building systems that were privacy-first instead of privacy-last. Some people worked in advocacy, making sure that the public understood what was at stake, making sure that parents asked questions about what was happening with their children's data.

All of it mattered. All of it pushed the entire ecosystem toward better practices. A company would see that another company had been certified privacy-first. They would realize that privacy was becoming a market differentiator. They would invest in changing their practices because investors cared about reputation and because other companies were getting certified. A district would see that another district had implemented privacy protections and had not experienced a loss in educational effectiveness. They would do the same, understanding that the good practices that worked elsewhere could work for them. A parent would read about data extraction in schools and would ask questions about what was happening with their child's information. A teacher would feel empowered to demand better contracts, knowing that other teachers had done so successfully. The pressure would build.

The ecosystem was shifting. It was shifting slowly, against enormous economic pressure. It was shifting against incentive structures that rewarded extraction and penalized protection. It was shifting against venture capital models that required exponential growth and data exploitation. But it was shifting. The pressure was mounting. The alternative ways of doing things were becoming more visible. The people doing the work were becoming more visible. Change was possible.

In March of year twenty-four, Maya was invited to speak at a tech policy conference about the evolution of education technology regulation. The conference was held in Washington DC. It included policymakers and technology leaders and advocates and researchers. It was the kind of forum where change sometimes started to happen. It was the kind of place where if you said the right thing to the right person, you could change the trajectory of policy. It was the kind of place where powerful people listened if you had expertise and evidence.

Maya had been given a slot on the main stage. She was told she had thirty minutes. She was told there would be a moderator and then questions from the audience. She was told there would be press. This was visibility. This was a platform. This was a chance to say what she believed to be true to an audience that could actually change things.

She wrote her speech in the hotel room the night before. She did not use notes when she spoke. She had learned, over the years, that the most powerful communication happened when you looked people in the eye and told them what you knew to be true. When you spoke from conviction instead of reading from a script. When you spoke the things you had learned through thirty years of fighting these battles.

She talked about the Axiom case. She told the story of the discovery, the investigation, the prosecution. She talked about what had changed in the twenty-two years since. She talked about what remained to change. She talked about the Luminance system and what it represented: the next generation of the same extraction, dressed up in new language. She talked about the companies that were building better systems and the schools that were choosing to use them.

"The question that matters now," she said, standing at the podium, looking out at the room full of people who had power, who made decisions, who could move the needle, "is whether we're going to continue reactively addressing harms in education technology, or whether we're going to proactively create standards that prevent harm from happening in the first place."

"Reactive response is what we've been doing. We find a problem. We investigate it. We prosecute it. We create policy around it. It takes years. It requires victims to exist before we act. It requires harm to happen before we respond. We respond to the damage after it's done. We criminalize the behavior after children have been harmed."

"Proactive prevention means creating standards before problems emerge. It means requiring transparency and accountability as conditions of operating in schools. It means assuming that companies will extract value from student data and creating rules that make that extraction difficult. It means designing school systems where privacy is the default and extraction requires special justification. It means changing the burden of proof: companies have to prove they're not extracting value instead of schools having to prove that they are."

"The resistance to proactive prevention is always the same: it stifles innovation. It costs money. It makes it harder for companies to operate. It slows down the development of new technologies. All of those things are true. And all of those costs are worth paying if the alternative is allowing student data to be exploited."

She talked about the privacy-first certification program. She talked about the companies that were choosing to meet higher standards. She talked about the evidence that privacy-first systems could still be effective and could still be profitable. She talked about schools like Cascadia that had chosen privacy protection and had not seen a decrease in educational outcomes. She talked about the fact that the choice was not between good education and privacy protection. The choice was between ethical and unethical. Between systems that respected students and systems that exploited them.

"The ecosystem is shifting," she said. "It's shifting slowly. But it's shifting. Some companies are understanding that privacy is a competitive advantage, not a constraint. Some investors are understanding that there are profitable business models that respect privacy. Some school districts are understanding that what matters is not just whether the technology works, but whether the technology respects the people using it."

The speech was well-received. There was applause. There were people coming up to her afterward with questions and comments. There were policy people telling her that her framing had helped them think about the issue differently. There was a venture capitalist telling her that he had not realized that privacy-first systems could be profitable. There were school administrators asking her how they could start building privacy protections in their own districts.

After the speech, a reporter from a major tech publication asked to interview her. They met in a coffee shop near the conference hotel. The reporter was young, maybe thirty, smart, asking good questions. This was a chance to shape the narrative. This was a chance to make sure that the work was visible.

"I'm interested in how you went from being a data forensics consultant to being an institutional advocate for privacy," the reporter said.

"I didn't go anywhere," Maya said. "I stayed in one place and that place's problems got bigger and more visible."

"But you could have done much bigger work," the reporter said. "You could have founded a company. You could have become a policy advisor. You could have done something national or international. Why didn't you?"

"I could have," Maya said. "But I don't think that would have been more effective. I think the most effective work happens when you actually have skin in the game. When you're responsible for outcomes. When you have to live with the consequences of your decisions. When you can walk into a classroom and see the student who is being protected by the policy you fought for."

"Don't you get frustrated by the pace of change?" the reporter asked.

"Yes," Maya said. "All the time. Every single day. But I'm also realistic about what change takes. I'm realistic about the fact that institutions are hard to change. I'm realistic about the fact that systems that are designed to extract value are very good at extracting value and very resistant to change. I'm realistic about the fact that changing an entire industry takes decades, not years. You don't change systems by waiting for the perfect moment. You change systems by creating sustained pressure."

"So I stay in my institution. I keep pushing. I keep supporting people who are trying to do better. And I trust that if many people are doing the same thing in their own contexts, in their own schools, in their own companies, the entire ecosystem will eventually shift."

The article came out a week later with a headline: "The Unglamorous Work of Protecting Student Privacy." Maya was amused by the characterization. It was accurate though. The work was unglamorous. It was bureaucratic. It was slow. It was often invisible. No one celebrated her when she prevented a bad contract from being signed. No one knew that a data extraction had been stopped. The success of her work was the absence of harm, and absence is hard to see. Absence doesn't make headlines. Success in this field was the thing that didn't happen, the problem that was prevented, the exploitation that was blocked. The harm that was avoided.

But it mattered. And she was okay with that being enough. She had learned long ago that impact didn't require visibility. That the work that changed the most was often the work that nobody noticed. The work that shaped institutions from the inside was invisible work. It was the plumbing of change. You didn't see it or think about it until something went wrong, until the system failed. But if the work was good, you never saw it. If the work was good, the system just worked. The privacy just existed. The students just were protected. And no one had to think about who had fought to make that possible.

That was okay with her. That was more than okay. That was exactly what she wanted.

In her office at Cascadia, Maya had a poster that had been given to her by the Principal of Newton Elementary. It showed a picture of a river flowing through a canyon. The canyon was immense, the walls rising up hundreds of feet. The river was small compared to the canyon, but its waters had carved the stone over millions of years. The caption read: "The river does not ask the canyon to move. The river moves the canyon."

It was a nice metaphor for what she was trying to do. She was not trying to convince institutions to change all at once. She was not trying to convince companies that privacy was good through some sudden moral reawakening.

She was trying to create sustained pressure for change, flowing in the same direction, wearing away resistance over time. She was trying to be the river. She was trying to keep pushing, year after year, decade after decade, until the system moved. Until the resistance gave way. Until privacy became normal.

It was slow. It was patient. It was the work of understanding that some things cannot be rushed, that some changes take decades, that the most important work is often the work that no one notices because it becomes normal. The work that becomes invisible because the good outcome is the norm. The work that shapes reality but doesn't announce itself. The work that you do because it matters, not because anyone is watching.

She had become a person who made student privacy normal in a school district. She had helped other people make it normal in their schools. She had helped create standards that made it normal across the industry. She had helped build an ecosystem where privacy protection was becoming the expectation instead of the exception. It was quiet work. It was ordinary work. It was the work that shaped reality from the inside, one contract at a time, one policy at a time, one student at a time.

And sometimes, late at night, when she was reviewing contracts or preparing for a meeting with a vendor, she would think about how far they had come. How different things were from when she started. How there were now five hundred Chief Data Officers across the country. How there was now a field. How companies were now choosing to get privacy-first certified. How students were now learning in districts that cared about their privacy. How the default was shifting, slowly, from extraction to protection.

It wasn't finished. It would never be finished. But it was different. And the difference mattered. And that difference was because people had stayed with the work. Because people like her had decided that this was the thing they were going to do. Because people had said no. Because people had built systems that respected students instead of exploiting them.

She was part of that. She was a small part of it, but she was part of it. And that was enough. That was everything.

The work of protecting student privacy was the work of patience and persistence. It was the work of saying no repeatedly until the system learned to hear it. It was the work of building relationships with vendors so they understood that you were not going to approve bad contracts, and they had to do better. It was the work of supporting the people around you who wanted to do better, who understood what was at stake, who were willing to fight the same fight.

Maya had become the person who did this work. It was not a role she had chosen. It was a role that had chosen her. She had seen a problem and had not looked away. She had understood what was at stake and had not moved on. She had decided that this mattered, and she had spent a quarter century proving that she was right.

The ecosystem that was emerging was not something that had happened by accident. It was something that people had built. It was something that required constant work. It was something that would disappear if people stopped fighting for it. But as long as there were people like Maya, like Delia, like the researchers and advocates and teachers and administrators across the country who understood that this mattered, the ecosystem would continue to grow. The pressure would continue to build. The system would continue to move, slowly, toward better practices.

Maya thought about the next generation of Chief Data Officers who were coming into the field. She thought about the young people who would read about the Axiom case and would understand that this was important. She thought about the students like Zara who would grow up understanding that their privacy mattered. She thought about the future when privacy protection would be so normal that people would wonder why it had ever been otherwise.

That future was not guaranteed. That future was contingent. It depended on people staying with the work. It depended on people saying no. It depended on people building better systems and refusing to accept less. It depended on people understanding that this was not just about data, but about student agency, about human dignity, about building institutions that could be trusted.

That was the work. That was the only work that mattered. And she was part of it. That was enough. More than enough. Everything that had any real meaning and consequence.

The Question

In year twenty-five, a student came into Maya's office. Her name was Zara, and she was a high school senior doing a project for her civics class about privacy in schools. She had requested an interview with Maya because she had heard that Cascadia School District had strong privacy policies. She had heard that there was a person in the district office who actually fought for student privacy. She had heard that things were different here. She wanted to understand why.

"I want to understand," Zara said, sitting down in the chair across from Maya's desk, her posture straight, her notebook ready, "how it became normal for schools to collect so much data on students. I want to understand why that's controversial. I want to understand why your district is different."

Maya thought about how to answer the question. She thought about the Axiom case and about how much had changed since then and about how much remained the same. She thought about Zara's generation, growing up in a world where data collection was the default and privacy was something you had to fight for. She thought about what it would mean to explain the history of that change to someone who had never known anything different. Zara had been in

high school her entire life in a district that protected privacy. That was normal to her. She had no frame of reference for what it was like elsewhere. She could not imagine a world where student data was extracted and profiled and sold.

"Schools collect data because data is useful," Maya said. "If I know that a student is struggling with algebra, I can give that student help. If I know that a student is thriving in a subject, I can encourage them to advance. Data makes teaching better. That part is true. Data is a tool. And like all tools, it can be used well or poorly."

"But my school collects more data than that," Zara said. She had clearly thought about this. She had clearly observed what was happening. She had clarity that many adults didn't have. She was noticing the things that should be noticed. "They collect data about which hallways I walk down. They collect data about what I eat for lunch. They collect data about what websites I visit on the school network. They collect data about how much I talk in class. They collect biometric data from the card readers at the door. I know because I've seen the contracts. I found them in the district website."

"Yes," Maya said. "Schools collect a lot of data. Most of it is not used for teaching. Most of it is collected because it's easy to collect, because vendors offer it, because it might be useful sometime in the future. Because no one is saying no. Because the default is to say yes to every data collection opportunity that comes along. The default is surveillance until someone makes it not the default."

"Is that bad?" Zara asked.

"It's not good," Maya said. "It means you're generating information about yourself that could be used to profile you, to predict your behavior, to influence you. It means you have less agency over your own life because you're constantly being watched. It means that decisions are being made about you based on data that you didn't know was being collected and didn't consent to being collected. That's not good. That's the opposite of good. That's the thing I've spent my life trying to prevent."

"What did you do about it?" Zara asked.

Maya told her about the work. She told her about reviewing contracts, about the meetings with vendors, about the moments when she had to say no. She told her about pushing back on vendors. She told her about saying no to systems that extracted too much data. She told her about the Axiom case twenty-five years ago, about the company that had built behavioral profiles on students without consent, about how that had changed her understanding of what was at stake. She told her about the moment she realized that no one else would fight this fight if she didn't, and the moment she decided to fight it.

She told her about the networks she had built, the standards she had helped create, the companies that had changed their practices because of pressure from schools and from advocates and from people who understood that privacy mattered. She told her about the difficult work of changing the industry from the inside, one contract at a time, one negotiation at a time, one district at a time.

"Did it work?" Zara asked. The question was simple but it held everything. Had the work mattered? Had things gotten better? Was it worth it?

"It worked partially," Maya said. "We collect less unnecessary data now. We're more careful about what we collect. But we still collect more than we probably need to. And there's always pressure to collect more, to use technology to manage and optimize student behavior. To track student movement. To predict which students will fail so they can be intervened on before they fail. To identify which students are at risk of dropping out. The pressure to extract is constant."

"Why don't you stop collecting data altogether?" Zara asked.

"Because teaching requires information," Maya said. "A teacher needs to know if a student understands the material. A teacher needs to know if a student is struggling. A teacher needs to know what a student's learning style is, what works for them, what doesn't. You can't teach well without information. Teaching is inherently a data-driven activity. The question is not whether to collect data but how."

"But also," Maya continued, "I'm not naive about technology. Data is going to be collected whether I like it or not. The technology is too powerful.

The incentives are too strong. The vendors are too sophisticated. The algorithms are too good at finding patterns and extracting value. The infrastructure for surveillance is being built whether we approve of it or not. The question is not whether to collect data. The question is how to collect it and use it in ways that are ethical and that protect student agency. The question is whether students know what data is being collected and have some say in how it's used."

"Is there a right answer?" Zara asked.

"No," Maya said. "There's just better and worse. This school district is better than many others. But it's not perfect. No system is perfect. Perfect would be not collecting any data about students, but that's not possible in a modern school. Perfect would be students having complete control over what data is collected about them, but that's not realistic when you're teaching large numbers of students. So we settle for better. We settle for less data. We settle for more transparency. We settle for more student agency. We settle for knowing what we don't know, knowing what harm might come, and trying to prevent that harm."

"Does that frustrate you?" Zara asked. "Having to do something that's just better instead of actually right?"

Maya smiled. "Yes," she said. "It does. Every single day. But I've learned that perfect is often the enemy of good. If you wait for the perfect solution, you don't implement the better solution. And the better solution, implemented now, is better than the perfect solution that might exist five years from now, that might never exist, that is always just out of reach. You have to live in the world of better, not the world of perfect."

"How did you get into this?" Zara asked. "How did you decide this was the thing you wanted to spend your career doing?"

Maya thought about that. She thought about the early days, the discovery of Axiom, the anger she had felt, the sense that something had to be done, the choice to stay and do it instead of moving on to something bigger or more prestigious. She thought about the moment when she realized that this was the thing that mattered, and that she could not turn away.

"I didn't decide," Maya said. "I encountered a problem. I was hired to audit a contract and I found something. I understood what the problem meant. I understood that it mattered. I understood that children were being profiled, that their data was being extracted, that their futures were being shaped by systems they didn't understand and had never consented to. And once I understood that, I couldn't turn away. I couldn't pretend not to see it. I couldn't walk away and let someone else deal with it. I could either do the work or live with the knowledge that I was choosing not to do the work. And I didn't want to live with that knowledge."

"So you chose the work," Zara said.

"Yes," Maya said. "I chose the work. And I've been choosing it for twenty-five years. And I'll probably choose it for another twenty-five years if my body will let me. Because once you understand what's at stake, you can't unknow it. Once you understand that student data is being exploited, you can't pretend it's not happening."

Zara left with a lot of information for her project. She had been a thoughtful interviewer. She had asked good questions. She had understood the complexity of the problem without needing Maya to oversimplify it for her. She had understood that there might not be perfect solutions. She had understood that progress mattered even when progress was incomplete. She had understood that doing the work was worth it even when the work would never be finished.

A month later, Zara came back to give Maya a copy of her project. It was titled "Surveillance in Schools: How Privacy Became the Responsibility of Districts Instead of a Right of Students." The title captured something true: that the responsibility for protecting student privacy had fallen to people like Maya instead of being built into systems and law. It captured the fact that privacy protection was something you had to fight for instead of something that was given.

In the conclusion, she had written: "The work of protecting privacy in schools is not finished. It will probably never be finished. But people like Maya Chen are doing the work of making it harder to exploit student data and easier

to respect student agency. This work is slow and bureaucratic and often invisible, but it matters because it shapes the institutions that shape our lives. It matters because it's work that respects the people being served instead of extracting value from them. It matters because it assumes that students are people first and data sources second. It matters because it builds a different future, one contract at a time."

Maya kept the project in her office. She read it whenever she was frustrated by how slowly change was happening. She read it when she was tired of the constant work of pushing back on vendors and creating policies and reviewing contracts. She read it when she wondered if the work mattered, if it made a difference, if it was worth the energy and the time and the constant vigilance. She read it and remembered why she did this work.

Zara's project reminded her that the work mattered. Not because it solved the problem completely. The problem would never be solved completely. But because it changed how the problem was approached. It changed from assuming exploitation was acceptable to assuming it needed to be justified. It changed from treating student data as a resource to be extracted to treating it as something that required careful stewardship. It changed the culture of the institution, which was slow and hard but was the only real change that lasted.

In the evening of the day she finished reading Zara's project, Maya went for a run. She was fifty-seven years old now. She had been running at five AM for most of her adult life. The run that had started as a way to clear her head had become something else over the years: a way to think, a way to process, a way to stay connected to her body and to the city and to the person she was. It was her meditation. It was her counselor. It was the place where she made sense of things, where she could think clearly about what mattered.

As she ran through the quiet streets, she thought about what twenty-five years of work had meant. She thought about the people she had helped. She thought about the systems she had changed. She thought about the vulnerabilities she had closed and the vulnerabilities that remained. She thought about the companies that had changed their practices and the companies that were still extracting data. She thought about the districts that had adopted privacy protections and the districts that were still letting vendors

do whatever they wanted with student information.

She thought about Zara, who understood at age eighteen what it had taken Maya decades to learn: that the work of protecting privacy was the work of respecting human dignity, and that it was worth doing even when the work was incomplete, even when the victory was partial, even when the change was slow.

By the time she got home, she had made a decision. Not a new decision. The same decision she had been making for twenty-five years. She would keep working. She would keep reviewing contracts. She would keep pushing back on vendors. She would keep supporting teachers and administrators who wanted to do better. She would keep saying no when she needed to say no. She would keep building systems and policies that made privacy the default instead of the exception. She would keep being the person in the room who understood the threat and who wouldn't look away.

She would keep showing, in one school district, that a different way was possible. And she would trust that other people, in other contexts, in other schools, in other organizations, were doing the same. And that slowly, over time, the entire ecosystem would shift. That the work would matter. That the slow accumulation of better practices would eventually become the norm.

She thought about Zara as she ran. She thought about what Zara's generation would inherit. They would inherit a world where student data was being collected more than ever before. They would inherit technologies that could extract more information, build more detailed profiles, predict more about student behavior. But they would also inherit a field of people who understood this. They would inherit standards. They would inherit the knowledge that this mattered. They would inherit the tools to fight back.

She thought about the choices Zara would make. Would Zara choose to do this work? Would Zara understand that the bureaucratic work of protecting privacy mattered? Would Zara see the unglamorous work as worth doing? Or would Zara be drawn to something bigger, something more visible, something that seemed more important?

Maya didn't know. But she knew that she had given Zara something. She had given her the knowledge that this fight was possible. She had given her the

understanding that institutions could be different. She had given her the example of someone who had stayed with the work and who had seen the result of that work.

That was what Maya was building. She was not building a solution. Solutions were impossible. But she was building the infrastructure for ongoing resistance. She was building the standards and the knowledge and the networks that would allow the next generation to continue the fight. She was building the understanding that this mattered, that privacy was worth protecting, that students deserved to be treated as people instead of data sources.

That was the inheritance. That was what she would leave behind. Not finished work. But work that mattered. Work that could be continued. Work that had shown that another way was possible. Work that had changed the landscape, slowly, persistently, in the direction of better.

She thought about how many Zaras there were across the country. She thought about all the students who were being protected by the work of people like her. She thought about all the teachers who were teaching better because they had better information about student learning. She thought about all the families who could trust that their children's data was being handled carefully.

The work was not finished. The work would probably never be finished. The work would be hard and frustrating and often invisible. But the work was good. And that was enough. That had to be enough. That was all she knew how to do and all she was going to do and it had to matter. And it did. It did matter. She could see that.

Epilogue: Five Years Later

In year thirty, Maya received a letter from the federal government. The Department of Education was establishing a new office focused on student data privacy. They wanted her to serve on an advisory board. They wanted her guidance on how to support school districts in implementing privacy protections. They wanted her to help them think about federal policy in ways that would not just regulate the worst actors but would enable the best practices.

She almost declined. She had been declining offers like this for years. Offers to move to DC. Offers to run national organizations. Offers to become a consultant for multiple districts. Offers to write a book. Offers to start a company. Offers to do the bigger work, the national work, the prestigious work. She had learned long ago that staying in one place and doing the work well was more valuable than chasing scale.

But this office was different. It was not about policy abstraction. It was not about creating rules from a distance. It was about implementation. It was about helping school districts actually implement privacy protections. It was

about working with the people in the trenches doing the actual work. It was about supporting the ecosystem that had emerged over the past thirty years. It was about staying close to the actual work while also helping shape the larger structure.

She agreed to serve. It meant quarterly trips to Washington DC. It meant meetings and consultations. It meant being part of conversations where federal guidance was being written. But it also meant working directly with federal agencies to support districts doing the work she cared about. It meant staying in Seattle and the work she was doing while also being part of the bigger picture. It meant not abandoning her district to become an abstract expert. It meant keeping skin in the game.

The Cascadia School District had fully retired her from her Chief Data Officer role the year before, but she had continued as a consultant. She was sixty-two years old. She was still running at five AM most mornings. She was still reviewing contracts. She was still working with teachers and administrators to understand what data they actually needed and how to protect the data they collected. She was still saying no to vendors who wanted too much. She was still pushing back on systems that extracted more than they contributed. The work had not changed. The work would not change. This was what she did.

She had learned that the work would not end, and that was okay. The threat would always be present. The temptation to extract value from student data would always be strong. New technologies would always emerge that promised to revolutionize learning and that threatened privacy. But the defenses would also continue to evolve. The standards would continue to strengthen. The ecosystem would continue to shift. There would always be more to do.

Delia Park had expanded the privacy-first certification program to international scope. Companies from Canada, the UK, Australia, and several other countries were adopting the standards. Delia had written a book about her experience as a whistleblower and as someone rebuilding the industry from inside. The book had been well-received. It had told the story of what had happened at Axiom, of the people who had tried to expose it, of the legal

battles, of the aftermath. It had shown that the work of changing the industry from inside was possible. It had shown that the incentives could shift if enough people pushed hard enough.

Daniel Kim's company had been acquired by a much larger education technology firm. The acquisition had been structured specifically to protect Daniel's ability to maintain privacy-first practices and to expand them to the other products in the acquiring company's portfolio. That had been hard-won. That had required negotiations where Daniel had been willing to walk away if the acquiring company would not commit to privacy protection. That had required leverage and knowledge and the willingness to turn down money if the money came with compromises he could not make.

Priscilla Holt had retired completely. She lived in the San Juan Islands and spent her time gardening and reading and occasionally consulting with districts on governance questions. She was ninety years old. She had been part of the original fight against Axiom. She had hired Maya. She had supported her through the early years. She had shown Maya what it looked like to be in a position of power and to use that power to protect the vulnerable.

Garrett Sable had served his eighteen-month sentence and was now living quietly in upstate New York, working as a consultant to help education technology companies avoid making the mistakes he had made. He had testified against the companies he had worked with. He had provided evidence about how data extraction worked, about the incentives that drove extraction, about what it took to resist those incentives. He had become a cautionary tale and a resource. He had become the person who understood from the inside how the system worked and how it could be changed.

Agent Marcus Webb had retired from the FBI. He had written a book about the investigation into Axiom and had become something of an expert on behavioral profiling systems and how they were used. He had become an advocate for privacy protections. He had brought law enforcement expertise to the conversation about how to detect and prevent data extraction. He had become part of the ecosystem of people fighting for privacy protection.

Maxwell, Maya's second cat, had given way to Schrödinger, a black cat with an uncertain temperament who was always either asleep or causing chaos, with no middle ground. Schrödinger had appeared at Maya's apartment one night and had decided to stay. Schrödinger did not negotiate. Schrödinger did not ask permission. Schrödinger simply was, indifferent to the world, and Maya was okay with that.

The Cascadia School District had maintained its leadership position on student data privacy. Other districts across Washington continued to adopt similar policies. The privacy-first certification program had become an industry standard. Federal guidance on student data privacy now referenced Cascadia's policies as best practices. The work that had seemed impossible thirty years ago was now becoming the baseline expectation.

In May of year thirty, Maya was invited to give the keynote address at a conference of Chief Data Officers. There were now over fifteen hundred of them across the country. The field that had not existed when Maya took her position now existed. It was professionalized. It had training programs and conferences and journals. It had standards and best practices. It had professional associations. It had career paths. It had become a real field.

Maya stood at the podium and looked out at the faces of people doing the work she cared about. Some of them had been in the field for twenty years. Some for five. Some for five minutes. They were all there because they understood that this work mattered.

"I was thinking about where we started," she said. "Thirty years ago, a school district discovered that a company had been collecting student data and using it to build behavioral profiles without consent. That discovery led to an investigation, a prosecution, and a series of conversations about what responsible data use looked like in schools."

"None of us in this room existed as a field when that conversation started. We existed because a problem had to be solved and we were the people willing to solve it. We existed because we understood that someone had to care about protecting student privacy, and if no one else was going to care, then we had to care. We had to step up. We had to be willing to say no. We had to be willing to

do the slow, unglamorous work of building systems that protected privacy instead of exploiting it."

"Some of you have been in the field for twenty years. Some of you for five years. Some of you for five minutes. But you're all here because you understood that protecting student privacy and enabling good teaching are not incompatible goals. They're the same goal approached from different angles. They're both about respecting students as people. They're both about building institutions that can be trusted."

"This work will not be finished in our lifetimes. There will always be new technologies that promise to revolutionize learning and that threaten student privacy. There will always be new vulnerabilities to identify and close. There will always be pressure to extract more value from student data. There will always be companies that see students as data sources instead of people."

"But we have shown that another way is possible. We have shown that you can have good technology and ethical practices. We have shown that transparency and accountability and student agency can be built into how schools use data. We have shown that the most important work is often the unglamorous work of sitting in a school district and reviewing a contract and having difficult conversations with teachers about what data they need and what they don't."

"It's work that will never make you famous. It's work that will probably never be easy. It's work that requires constant vigilance and constant pushing. But it is work that matters. It is work that protects actual students in actual classrooms. It is work that makes a difference in the lives of children."

"I'm going to keep doing it. I hope you will too."

The applause filled the room. She saw people taking notes. She saw people taking photos. She saw the young CDO from earlier approaching her with tears in her eyes, saying that she had found her calling, that she understood now why this work mattered, that she was going to spend the next decade doing it.

After her speech, that young woman approached her, maybe twenty-five years old, a Chief Data Officer in her first year in a mid-sized district.

"I was inspired by your work," the woman said. "I read about the Axiom case and I understood that this was the field I needed to be in. I wanted to tell you that."

Maya thanked her. She told her that the work was hard but important. She told her to stay connected to the actual impact of what she was doing. She told her not to let the work become too abstract or too policy-focused. She told her to remember that she was protecting actual students.

"Don't let them tell you that your work doesn't matter because it's local," Maya said. "Don't let them tell you that you're not ambitious because you're staying in one district instead of running a national organization. The local work matters. The work of protecting privacy in one school district matters because it protects actual students. And if enough people do local work in enough districts, the entire system changes."

That night, in her hotel room, Maya thought about what thirty years meant. She thought about the person she had been when she started: a data forensics consultant with a contract to audit a school district. She thought about the person she was now: someone who had spent thirty years building systems and policies and a field focused on protecting student privacy.

She had not set out to do this. She had set out to audit a contract. She had looked at the data and seen what was happening. She had understood the scope of the problem. She had understood that someone had to say no. And she had been the person in the room who could say no, who understood what the problem meant, who had the technical knowledge to see it.

Once she had seen the vulnerability, once she had understood the scope of what was being done, she could not unsee it. She could not turn away. She could not pretend it wasn't happening. She could not move on to something else and let someone else deal with it.

So she had stayed. She had stayed in a school district. She had stayed in the difficult work of building systems and policies. She had stayed when faster or more glamorous paths were available. She had declined the promotions that would have taken her away from the actual work. She had chosen the unglamorous path of protecting privacy one contract at a time, one policy at a

time, one district at a time.

And she had watched the entire field shift. Not because of her alone. Because of many people, in many places, who had stayed with the work. Who had understood that this mattered. Who had been willing to build systems that protected students instead of extracting value from them. Who had been willing to say no to companies that asked for too much. Who had been willing to do the slow, patient work of building better institutions.

It was a good thing. It was a good way to spend thirty years. It was a good way to spend a life.

She packed her hotel room the next morning and flew back to Seattle. The flight was full of people traveling for work, for conferences, for meetings. She sat by the window and looked out at the city as they approached. She could see the Elliott Bay. She could see the mountains beyond. She could see the neighborhoods where she had lived for more than thirty years.

She went home to Schrödinger and her apartment and the work that was waiting. She had contracts to review. She had teachers to advise. She had a field to help build. She had a world to protect. The work was there, waiting for her, the way it always was.

The work would never be finished. But that was okay. Some of the best work was the work that you never finished, the work that mattered more because it was ongoing, the work that required commitment and patience and the willingness to stay with something even when progress was slow. The work that required you to believe that what you were doing mattered even when you could not see the full impact of it. The work that required you to trust that if you kept pushing, if you kept saying no, if you kept building better systems, then eventually the entire ecosystem would shift.

She had been staying with it for thirty years. She would probably stay with it for thirty more if her body would allow it. Because the work mattered. Because she could see, every day, that it was making a difference. Because students were being protected. Because families could trust that their children's data would be handled carefully. Because teachers could understand what data they actually needed to teach well.

And because sometimes, the most important thing a person could do was to stay in one place and make that place better, knowing that if enough people did the same in their own places, the entire world would eventually change. Not quickly. Not easily. But it would change. And that was worth everything.

The run that morning was cold. There was light snow on the ground. By five fifteen AM, the sun was starting to come up, and the city was beginning to wake. Maya ran through the neighborhood where she had lived for more than thirty years, past the coffee shop where she had first met with Tomás all those years ago, past the grocery store where she bought food for her cat, past the school buildings where thousands of students would spend the day learning.

Data on those students was being collected. Profiles were being built. Decisions were being made about what they needed and what they were capable of. Vendors were pitching systems that promised to revolutionize learning while extracting enormous amounts of data. Teachers were trying to figure out what tools to use, what to trust, what to resist.

But those decisions were being made more carefully now. The data was being protected. The students had more agency. The teachers had more control. The parents had more information about what was being collected and what it was being used for. The institutions were different. The systems were different. The defaults had changed.

It was not perfect. It would probably never be perfect. But it was better than it had been. It was better because people had stayed and fought. It was better because people had said no. It was better because people understood that privacy mattered and that the protection of privacy was a responsibility they could not shirk.

It was worth fighting for. It was worth thirty years of work. It was worth a lifetime of commitment. It was enough. It was more than enough. It was everything that mattered.

The sun was coming up now, the city beginning to wake. She could see the first light touching the tops of the buildings. She could see the city stirring, preparing for the day. Thousands of students would go to school. Thousands of students would have their data collected. Thousands of students would be

protected, a little bit better protected than they would have been, because of the work that people had done.

That was what it meant. That was the only thing it had ever meant. The work mattered because students mattered. The protection mattered because students mattered. That was enough.

About the Author

Dr. Terry Oroszi is the founder and director of Mission Possible Spy Academy (MPSA) and Mission Possible Institute, based in Dayton, Ohio. A U.S. Army veteran, her career spans academia, federal consulting, and national security -- including research partnerships with the FBI, DHS, and DoD. Her published work includes The American Terrorist: A 20-Year Study and The Complete Guide to Open-Source Security. The MP SPY ACADEMY fiction series draws on the behavioral intelligence frameworks she designed for the MPSA 10-ribbon pipeline. Pro Bono Non Malo -- For Good, Not Evil.

Also in the MP SPY ACADEMY Series

Book Two in the MPSA series, "The Leverage," follows Maya as she faces the political fallout from exposing Axiom Learning Solutions, discovers connections between the shell companies and international intelligence operations, and finds herself in the unusual position of being simultaneously a whistleblower, a federal witness, and a consultant to the very people investigating her findings. Nothing goes the way anyone expected.