THE ORIGIN POINT
A Future Tech Cyber Novella
by Case Lane

Discover other books by Case Lane:
Angle of Deception
The Motion Clue: A Future Tech Cyber Thriller
The Unbroken Line: A Future Tech Cyber Thriller

Table of Contents

Novella Description

The Origin Point: A Future Tech Cyber Novella

Your Future is in Play

WITHOUT THE CONSENT OF THE GOVERNED two American federal government cabinet ministers involve the U.S. in a secretive alliance to create a global surveillance and online tracking system of sweeping control. But a ubiquitous flash drive with shocking content falls into the hands of an intrepid journalist, and the untold plan may suddenly be made available to

the world. When global cyber security is the prize in the race for our online future, can the defiance of two master operators backed by a clandestine global group outpace the vaunted skill of America's free press and an underground cyber defense team with its own agenda?

Who will win a contest of wills and intelligence when the only question asked is: do you want individual privacy or do you want global security?

This novella is the first prequel in the Life Online series of cyber thrillers about the future impact of our rising dependency on technology. To find out why we end up in a post-control world governed by the sophisticated software of an omnipresent server network, start here...

THE LIFE ONLINE BOOK SERIES

YOUR FREE COPY IS WAITING

From the author of the Life Online Book series, **The Power of Preparation: 10 Things to Do Before the Future Arrives** is a free guide to help you learn about the steps to take today to be ready for tomorrow.

Click here to get your free copy
OR
Go to Case Lane's website and click Send My Free Copy

The Origin Point: A Future Tech Cyber Novella
Prequel 01 in the Life Online series

PROLOGUE

Easter Sunday morning, 2014

The glaring lights illuminating from the pedestrian plaza in front of the White House in Washington, D.C. provided Elmira Sanchez with a luminescent bath as she diligently finished cleaning inside Infrared, one of the city's most exclusive restaurants. D.C. was a power town and even at 3 am, the vivid intensity of the streetlights marking the pedestrian pathways and sidewalks around one of the world's most significant buildings, enveloped the plush chairs and white table-clothed dining tables around which she was maneuvering an industrial vacuum. In the past year, the city's influence peddlers from brokers to senators to lobbyists to lawyers to journalists to financiers to diplomats had turned Fresno Tyler's early American eatery into a go-to location for intimate conversation. The low-walled booths lining the walls around the restaurant were self-contained sanctuaries for a discerning few who preferred to slurp through their cumin-infused wheat flakes and cayenne chewy bacon, in splendid isolation from the sight of their enemies.

Sanchez had no time to think of the guarded discussions that had taken place hours before she arrived. Her crew cleaned four restaurants around the neighborhood between midnight and 8 am each night. For them, Infrared was a building space where grease in the kitchen and tissues in the toilet had limited impact on their senses. They learned to ignore the sights and smells encircling their bodies while sweating through the late night tasks. As overnight patrons occupying the restaurant space, the cleaning crew were not engaged in billion-dollar policy negotiations to change the laws of America, but were wiping away the discarded food and human waste made unimpressive by indulgence and decay within each location where they worked. The media-created cachet linking the exclusivity of being inside Infrared to the privileged few, failed to consider the $12-an-hour cleaners with children to feed who were also among the restaurant's recurrent guests. But the workers knew the five star menu did not reduce the smell in the bathroom when a power broker decided to occupy a stall as if he were at home. Nor could a reservation waitlist stretching over ten months upgrade the chore of removing rotting animal flesh, fruit and vegetable cast-offs, and buckets of grease from the premises each night. The vision of Infrared captured in its kitchen and bathrooms revealed not a must-see destination of pounding conversation and emotion, but a soiled, misused, crowded functional space, requiring by law, a complete refreshment each night before the cycle could begin again the next day.

Turning the vacuum around a corner, Sanchez's eye caught a sparkle of silver shining from a ledge next to a table. Normally, she would be indifferent to any item not in her immediate cleaning area, but Tyler was meticulous about the cleanliness of his restaurant, and had demanded the crew immediately report any maintenance issues such as peeling paint or torn carpet so he could address the problem before a dining guest noticed the flaw. Since the cleaning service was outsourced to another company, Tyler paid extra for the vigilance, and Sanchez's supervisor enforced the additional attention.

Knowing Tyler would inspect the restaurant as soon as their work was done, Sanchez reached for the object. Picking the piece up, she realized only the end was silver, the rest was a dark blue plastic. Looking at the item between her fingers, she recognized the two-inch device, but could not recall the object's common name. The silver end, she knew as 'the thing you save computer files onto when you want to move them to another computer.' A friend had once handed her a similar looking gadget when she was giving her pictures of her daughter's birthday party. 'She called it a stick,' Sanchez remembered, amused. 'A memory stick.' Briefly considering again if the name was correct, she put the stick in her pocket, and continued with her rounds.

An hour later while preparing to leave, Sanchez spotted Tyler in his office staring at his computer screen and was prompted to recall she was carrying the memory stick. With a slight nervousness, she lightly knocked on Tyler's open office door. The restaurateur looked up.

"Yes?" Tyler asked without emotion. Razor-thin with curly blond hair and bright green eyes, Fresno Tyler had exited the tranquil rural New York state town where he had been born and raised to change his name, learn to cook and hustle his ambition up the ladder of restaurant success. Infrared was his third location, the first in D.C., conveniently built in a well-trafficked neighborhood, after an influential political party backer tasted Tyler's signature beef pasta one evening at his first New York City spot, and offered to buy him a retail space to establish a franchise in the nation's capital.

"*Señor* Fresno," Sanchez said removing the stick from her pocket and holding the item up for Tyler to see. "I found this." Lightly walking towards him, she reached out her hand to offer him the memory stick.

Tyler furrowed his brow and stretched out his palm, Sanchez dropped the piece onto his hand. "What's this?" he asked to no one in particular.

"It was by a window, a table in section 3," Sanchez offered.

"A flash drive?" Tyler patiently inquired, looking at the stick. Sanchez shrugged but did not respond. "Oh, okay thanks." Sanchez nodded and walked out.

Without watching her depart, Tyler turned the flash drive over in his hand. The device was unmarked, no name or even a brand logo appeared on the plastic casing. Shrugging, he placed the silver end in his laptop's USB slot and opened the document view. He looked first for any sign of the owner's name, but no identifiers were prominently displayed. The files, however, were all visible, not encrypted, nor locked using a password. Each file was named for a current issue facing the American people - discrimination, public education, law enforcement, consumer protection. Tyler clicked open the discrimination file. He checked the 'properties' feature for an author's name, but the fields were blank. Glancing back at the content of the file, he presumed the information was a thought-piece. "Preventing the next Dr. King or Ms. Steinem from gaining a foothold," Tyler read the document title aloud. "Sounds sufficiently ominous." As he continued to read in silence, he noted the scope of the document's ideas were laid out as policy or planning instructions for the future.

In Washington, a policy document could originate with anyone from the President's Chief of Staff to a mid-level civil servant to a student summer intern at a think tank. But even to Tyler's untrained eye, the document, with its detailed strategy and references to senior government leaders was too meticulously prepared to be a random discussion piece. The content looked...like official federal government documents. Tyler opened another file. Searching 'properties' again, he confirmed there was no identifying information. But similar to the first document, the content appeared to be laying out the parameters for the organization of America's

future.

'Where did this come from?' he wondered. 'Who was mapping out these ideas in such detail?' Knowing his continued speculation would be fruitless, he sent a text to his friend Dallas Winter, a journalist at the National Republic. 'If anyone could uncover the source of these files,' he thought. 'She could.'

A few blocks away, Dallas was asleep when her subconscious picked up the chime for a message alert on her mobile phone. Mechanically she reached for the device, and viewed Tyler's request for her to look at the government documents he had found. Immediately, she hit the 'call' icon.

"You found what?" Dallas asked, the second Tyler answered on his end.

"I'm so happy you stay up all night," Tyler replied. "Especially when I cannot decipher mysterious government files."

"I was not awake. Why do you think you found government files?" Dallas yawned through the question. "This is D.C. Everyone is writing about what they think the government should do."

"The detail is intense, full of names of real people who are actually in a position to do these things."

"But still, extra detail doesn't mean—"

"Look, can I drop the drive off on my way home? I really do not want unclaimed government documents in my possession when the feds show up."

"What am I supposed to do with a lost flash drive?"

"Figure out who the files belong to. If it's just some kid at a think tank, you can be a Good Samaritan and return the documents to him. If it's one of the political parties, you can sell the information to the other one. Or if it's government leadership and they're up to something, you've got yourself a story."

Dallas considered the options for a few more seconds. "Okay, I'll put some clothes on."

"Oh no, please don't bother."

"Very funny."

"I'll see you in a few minutes."

Tyler exited the restaurant through the back entrance, setting the alarm as he went. His Mercedes sports coupe was parked in the underground garage of an adjacent building. Stepping into the brightly lit alleyway, he crossed from one door to the next and began to descend the stairs. Despite D.C.'s reputation as a crime shaken city, the streets encircling the White House had an additional layer of surveillance cameras, and enough lighting wattage to ensure the area always appeared to be celebrating Christmas even in the middle of summer. Tyler did not think twice about wandering alone into a vacant alley or accessing his car from an empty lot. No crimes were ever reported around his restaurant, not even a pickpocket, such was the comfort provided by omnipresent electronic eyes.

Tyler lifted his key fob to open his car door. As he walked towards the side of the vehicle, he briefly looked at the reflection in the window, and caught the shadowed sight of a stick figure passing behind him. He stopped and carefully looked at the window glass for confirmation of his observation. But from his position, he could not clearly see completely around his surroundings. After waiting another minute to determine if the view in front of him would change from a blurred vision of the parking garage to the clear outline of another human, he rapidly turned around.

The parking lot was empty. Tyler looked left and right, but no person was visible.

'Okay now I'm getting paranoid,' Tyler thought as he jumped into the car. 'I really believe I'm holding wanted government documents. I need to chill out.' As he talked himself down from a moment he suddenly refused to consider as valid, he hit the starter button and raced out of the lot and on towards Dallas's apartment building.

Dallas lived in one of D.C.'s most convenient but expensive neighborhoods, Mount Vernon Square on the other side of Mass Ave from Chinatown. If America's capital had a downtown defined by bars, restaurants, and a sports arena, then Chinatown, complete with the obligatory friendship gate and signs in Chinese lettering, was downtown D.C. If one walked south towards the National Mall the tourist friendly dining choices gave way to stately office complexes designed for Roman Emperors. Venturing north past the homeless people sleeping in neighborhood parks, the commercial district's streets turned residential as new condominium towers were being erected in every direction to pull a moneyed class of young professionals, lawyers, publicists, lobbyists, thinkers and marketers, into the city's core. 'In a few years this will be a densely populated magnet neighborhood,' Tyler thought as he considered the growth potential for his restaurant business. 'D.C. will finally get some traction as a city of professionals who do not disappear into the suburbs each night, but stay to take advantage of the electric moving pace funded by national party politics, 24 hours a day.'

Instantly calmed by the thought of more patrons for his popular establishment, he parked in the street in front of Dallas's building and indifferently exited the car. Turning away as he lifted the fob to lock the door, he glanced at his window, and once again caught the unmistakable outline of a figure looming behind him. Bracing his hands on the car roof, he briefly closed his eyes. 'Relax Frez,' he silently told himself, before opening his eyes and slowly turning around. He was alone. Scattered sounds of laughter, glows of cigarettes, and insomniac dog walkers prevented the somber street from being wrapped in silence, but no figure was clearly visible within a near distance to where Tyler stood. Behind him was empty asphalt leading to more high-rises, the glare from signs of closed restaurants, and the glass windows of a 24-hour pharmacy. But he saw no humans or a lurking beast ready to pounce upon him and demand the details of all he knew. Tyler shook from head to toe. 'Get a grip,' he again admonished himself before hurrying towards Dallas's building door and buzzing for entry.

Opening the door to her apartment, Dallas greeted him in pajamas and a half-open robe. Her uncombed hair hung entangled to her shoulders, and without makeup, her face possessed the healthy youthful glow Tyler had admired since the day they met twelve years earlier, in his first New York City restaurant. "Wine or coffee?" she offered as Tyler entered. Without answering he went to the window and looked out into the street. "What are you doing?"

Still facing the view through the window, Tyler stated, "Okay I know this is going to sound like a super paranoid dude who is actually making up a backstory for the reason he came over here tonight, but..." he turned to face her, "...I think someone is watching me."

Dallas grinned. "Oh c'mon," she replied with a slight hint of concern. Dallas had never seen Frez Tyler operate in fear. His relentless drive was created from an indomitable courage designed to ensure he succeeded in an abrasive competitive world. Having been friends since she had encouraged him to invite acclaimed restaurant critics to try his back-to-the-farm food, she tried to parallel his approach to life. She too sought to be unsurpassed in her field and matched her progress towards prestigious reporting assignments, with his restaurants' rave reviews in the national media.

"I'm serious, Dal."

"You watch too many spy movies."

"I don't watch spy movies. Someone was watching me."

Dallas moved towards the window and observed the shrouded neighborhood below. "There is literally no one in the street."

"I saw something."

"Maybe a fan was trying to speak to you. You are a celebrity you know. Maybe someone knew who you were, but was too shy to ask for your autograph." Surprised, Tyler looked at her as if reevaluating his initial reaction. He never considered himself a celebrity. As a chef, he was driven by his ideas for creating healthy, tasty meals based on the cultivated cereals and domesticated animals humans began consuming when nomadic life ended 12,000 years ago. "Okay?" Dallas asked, as he appeared to settle down. Tyler nodded. "You work hard and have long hours. It's late. Show me the flash drive so we can both get some sleep."

Tyler slowly removed the drive from his pocket and handed the plastic stick to Dallas. She went over to her desk, turned on a light and put the drive into her laptop's USB slot. With one eye on the window, Tyler sat down on her couch to wait.

More than fifteen minutes went by before Dallas looked up at him with undisguised shock. "Frez, these are actually serious planning documents," she finally commented.

"I told you. With those details, I don't think the policies are some think tank's speculation," Tyler responded.

"No, I mean really serious. I think these documents were commissioned for FedSec."

"Very funny. You want me back to believing I am being followed?"

"No, I'm serious."

"Don't mess with me," Tyler admonished her, as he stood to walk towards the desk.

"I'm not kidding."

"You think these documents came from the Federal Security Commission? The government's top secret upon top secret 'who-knows-what-they-really-do' security agency? How could you know these are FedSec documents?"

"It's the template, the organization and style of the writing and the presentation. The documents read like their material."

"But the content is not FedSec's supposed mandate."

"I know. Look at this piece stating tech companies can code racism and sexism into their websites."

"Yeah I read that."

"They can prevent people from getting services, but easily deny the practice because there is no record."

"Yeah, completely illegal."

"And this one on weaponizing civilian law enforcement drones. Could you imagine if drones with guns were patrolling the streets? How could that be safe? Some of these plans are mapped out in detail, like how police forces could use the drones in urban neighborhoods. No word on doing the same thing in suburbia of course."

"No, of course not. But are you sure these documents could be FedSec?"

"Yes, this is exactly how they would present internally created material."

"Really?"

"Yes, I'm completely serious. I've been reading FedSec's documents for years. These files follow their templates to the letter. I mean people can copy a format, but another government department or a think tank would use a different style. No one is going to copy FedSec's document writing directives. Plus there's a tracker file on this drive."

"A what?"

"A tracker file. Whoever lost the stick can trace its location."

"What! Are you serious? Turn your computer off!"

"Frez, calm down. The tracker is off. That's probably why the drive was sitting in your restaurant. Someone left the stick there, but did not come running back to reclaim it because the tracker is turned off."

"Why would someone go to the trouble of adding a tracker file but leave the function turned off?"

"I don't know?"

"Okay what do you think these documents are for?"

"The content is obviously some future planning stuff, ideas about mapping out our online activities. These types of discussions are pretty commonplace these days. But the question is, who was in your restaurant tonight? Why did they take the drive out and how could they forget to take the documents home? All are marked 'top secret' and 'confidential.'"

"Yeah, you think someone would have come back."

"Unless they wanted the drive to be found by a third party."

"By me?"

"Why not, you're as good a whistleblower as anyone."

"Whistleblower? I don't blow whistles. I run a restaurant."

"Well maybe they thought you'd call one of your journalist friends."

"You think?"

"I don't know."

"Okay well either way, what now?"

"I'll investigate, try to find more information about the content. These files all cover a different subject, but I'm not sure if the details are leading to a bigger story."

"Like?"

"These documents are talking about integrating online activity across everything we do, putting all of the consumer tools together with surveillance from cameras and satellites."

"Sounds convenient."

"No, sounds like a gross invasion of privacy."

"Oh."

"In the name of national security."

"Ohhh...okay. How are you going to find out more?"

"The best way I can. I'll go right to the source and ask FedSec what they're up to."

*

CHAPTER ONE - THE DISCRIMINATION FILE

Appointments to meet with FedSec Director Marco Manuel usually had to be scheduled at least six months in advance and preferably a year. "Tell him I have a document I would like to discuss," Dallas politely explained to the Director's assistant. "Tell him the document title's first line is 'Preventing the next Dr. King or Ms. Steinem from gaining a foothold.'" The assistant noted the file name and placed Dallas on hold. A minute later, she hastily connected her to the

Director.

"Dallas, what's going on?" Marco jovially answered. A decorated soldier, seasoned political operator and runway-ready male statue, Marco had lines of supplicants panting at his door. Government officials sought his input and analysis on a range of issues from last second developments in conflict areas overseas to the outcome of football games; current, former and potential mates requested dinner and party appearance confirmations; assistants ran in and out of his office with documents to sign and updates to read; but he put all attendants on hold to respond to Dallas's incoming call.

"I have my hands on some interesting documents," Dallas replied. "And I would like your comment."

"What do you have?" Marco unemotionally inquired.

"Your policy papers."

"My policy papers?"

"Yes sir."

"What is the full title of the document you told my assistant about?"

"Preventing the next Dr. King or Ms. Steinem from gaining a foothold: Hiding race and gender bias in website code." Silence followed. "Mr. Director? Marco?"

"I don't even understand the meaning of those words," he carefully responded.

"The document appears to be a policy piece. Seems to be about the ability of businesses and governments to use computer code to put gender and race discrimination into the functionality of their consumer-facing websites."

"I still don't get the point."

"It's illegal."

"And how is this type of activity related to FedSec?"

"Well the policies appear to have been created by FedSec. I could show you the documents."

"Why would FedSec produce a policy paper on those themes? We do not deal with race, gender, or computer programs."

Dallas paused. "Well not directly."

"Not specifically at all. I'm sure you are mistaken, Dal. Sounds like the document could have come from anywhere. Guess you best move on. I doubt you have my policy papers, and I have a ton of work to do..."

"Marco wait, c'mon we are old friends," Dallas clearly stated. "If you do not recognize the title of the document why did you take my call?"

"Because we are old friends, and the title of the document was intriguing."

"Do you recognize the title from another department's work?"

"No. Like I said, I do not even understand the meaning."

"Can you recommend someone I can talk to about this policy?"

"The Department of Race and Gender Bias?"

"You mean the entire federal government?"

"Funny. But no, I mean talk to whoever you want but not to me because I'm a busy man."

"Marco...Mr. Director, these documents were clearly written following FedSec's policy template. I recognize the style."

"Well there's an interesting skill."

"I'm pretty sure I'm not the only one who has mastered the ability to determine the difference between documents produced by the various government departments. If I show this

document around town, other people will tell me the style is FedSec."

Dallas perceived a contemplative pause emanating from the other end of the secure landline. After an extended moment, Marco slowly stated, "Dal, do not show documents around town that you are claiming were written by FedSec. I'm sure the assertion would be a violation of one of our national security directives, and we do not want you to get into trouble."

Stunned, Dallas asked, "A violation of a directive? If the documents are not yours and I speculate they are, you'll just have a misled journalist in your midst. Why would my actions be an issue?"

The silence returned, but after a minute, Marco acquiesced. "All right, I'll take a look at these documents you have. Before you show the files to anyone else, bring them to me and I'll do the vetting."

"Great, thank you, but are you saying the documents could be yours?"

"No. You said the files were written using a FedSec template. I might be able to determine if another department has copied our template. And you should research on your side if a think tank or university is claiming knowledge of these topics. You are still going to have to figure out who created the documents."

"You're certain these policies were not prepared by FedSec?"

"Yes, I'm certain."

"Do all FedSec policy papers go through your office?"

"Yes, I'm the director. An employee cannot claim FedSec has a policy on an issue unless I approve the content first."

"How does your approval process work?"

Marco sighed. "The short version is everyone has a specific mandate, an employee proposes research in an area, the research is approved, the work is completed, the document comes to me and I sign off."

"So if these are FedSec documents, you signed off?"

"You are not holding FedSec documents."

"But if I were..."

"Dal, I do not have time for this back and forth. I'll send a team to pick you up, and you can bring me the documents and show me the information you claim came from this department."

"Wait. What? You'll send a team for me?"

"Yes."

"Why? What team?"

"I'm the director of FedSec, Dal. You cannot walk in here to have a chat. Electronic devices have to be vetted, you have to be vetted. A team is coming for you. When I authenticate digital devices, we move over to a more secure location."

"More secure? Why can't we meet in your office?"

"What did I just say? Civilians do not walk into FedSec and hand documents to the director. We will meet in a secure location."

"Just a second, Marco," Dallas pleaded, her voice rising in panic. "Do not put me through some weird secret spy stuff. Let's meet like normal people."

"I'm not normal people, Dal. Who did you think you were calling?"

"I know who I called."

"Good. You want me to authenticate documents on an electronic device, you have to follow my security protocols. The team will be with you in about an hour, and I'll be able to give you ten minutes. Someone will contact you. Cooperate and I promise the process will work

smoothly."

"Marco, you're kind of...kind of scaring me here."

"Don't worry, that's not my intention. Wait for the team and I'll see you soon."

*

"What do you mean a reporter may have the 2100 policy files?" United States Secretary of State Julia Davenport demanded to Marco over a secure phone line between their Washington, D.C. offices.

"As I said," Marco replied. "I am not 100% sure, but she had the full name of the discrimination file, you know the title invoking Dr. King and Ms. Steinem."

"Yes, yes I know the title. But how could she have learned about the file?"

"I'm going to find out."

"Isn't bringing her to meet you at Horizon a little suspicious?"

"No, she will have no idea about the location's actual use."

"The location is actually used for a non-existent organization."

"I am aware."

"We do not take reporters there."

"I will for checking a suspicious flash drive. I cannot speak to her in my FedSec office or at my home or worse, in a public place. As you are well aware, very few people know I have two jobs. FedSec by day, GCS by every other minute of the day."

"I also have two jobs, Marco," Julia dryly noted. "I'm in charge of State and GCS. But Global Cyber Security is the primary role dominating my life right now. We need a global cyber security defense, and this government will never have the mandate or the ability to deliver as our private interests can."

"I know," Marco responded. "I am completely with you. We are working around our own government to avoid the destruction of our national security and the ruin of our way of life."

Both the State Department and FedSec had the immediate need for a steadfast cyber security action plan near the top of their issues list. But underscoring the struggle between measured government and impatient influencers focused on parallel goals, Julia and Marco had collectively made a decision to continue as federal government cabinet ministers while moonlighting in the veiled outsider organization known as GCS, the acronym for Global Cyber Security.

GCS was a secretive global group with its own resources, which could ignore the government's plodding legislative approach to an omnipresent cyber threat, and focus on managing the demands of its financial backers who did not trust, nor wait, for governments to implement valuable directives in an efficient, rapid or permanent manner. With the option to work within the bureaucracy or outside with private interests, Julia and Marco chose both, and aligned to face the task of building a permanent cyber security blanket using every resource available. They intimately knew the nation desired a standing cyber defense force against online terrorists to functionally match the vigilance performed by physical soldiers guarding the air, sea and ground. At the same time, they recognized GCS's intent to create an infrastructure for maintaining an independent cyber security umbrella shielding America, and other valuable global markets, from internal and external saboteurs. Together, they determined to definitively accomplish the latter more accessible goal, while managing the former with strained patience.

Officially, within the State Department, cyber security obligations expanded in context with world events, which were upended each day whenever news of a cyber attack was announced. To address the subject with immediacy, in the quiet reaches of a somber Washington away from the lights of the media's issue-of-the-day publicity, a half dozen policy representatives focused

exclusively on recommendations for the continuous update and redesign of the nation's cyber security requirements. But similar to the country's last century determination to build an interstate highway system transcending a vacationer's desire for a road-trip; the interstate cyber security system had national commerce, global trade, defense, judicial, internal security, employment, and consumer implications. And when policy requirements touched every inch of the domestic agenda, all federal government departments jostled to weigh in on the proposed solutions. The cyber protection list grew from managing the federal government's digital infrastructure to include, helping private businesses avoid cyber attacks; monitoring online businesses operating in regulated industries or providing government services; utilizing personal digital information in law enforcement; and creating legislation for online privacy and personal data use.

After each external attack on government or business servers, technical investigators would converge on the damaged site and try to identify the vulnerabilities. But no overall comprehensive approach existed to compare the attacks and share findings across industries. Threat assessments were guesses based on the business's global profile and national prestige. The wealthier the company's resources, the more high profile the chief executive, the more envied the employees...the greater the chance of a backlash from independent hackers displaying their skill, not to impress the world, but to overwhelm one another with their daring. All law enforcement agencies struggled to learn more about cyber criminals who were out of reach from traditional investigative tactics, and working far-removed from their targets. But with each development forward, a setback emerged, sending the crime fighters scrambling for more information, answers and solutions where only questions remained.

Unofficially, to meet the cyber defense challenge outside the parameters set by government departments, unelected private GCS interests were in a relentless search for those who aligned with their intentions and sought to build their own confidential teams from the ranks of government, business, academia, non-government, and science and technology specialists who were willing to assist in defining control for their own preparation against cyber terror. People who were promising strivers in every field could facilitate the implementation of GCS's plans. Several individuals focused exclusively on finding like-minds and invited them to join the group's efforts, not through a meeting, but with demonstrating capability by accepting a task that if done correctly, solidified a position for the way forward. The invitation was not subtle. The selected knew the opportunity they were being offered could be a conflict-of-interest with the public role they held, but all accepted, because they also knew the world was in desperate need of cyber security leadership transcending the sound-bite demands of the news. For this group, the fact politicians had to play politics made elected leaders ineffectual for managing the volatile cyber threats of the future. They viewed politicians only as temporary representatives popularly elected to a manufactured seat of power from which their mandate was limited to one-liners addressing emotional societal issues. But the GCS group considered their self-proclaimed directive to be a more demanding task - to maintain the foundational fabric upon which those societal issues could be addressed.

Cyber security lay before them as an immediate issue requiring a long-term solution, one elected governments could not enact within their limited terms. Domestic dependency on the Internet provided enemies with a weapon of destabilization affecting government, businesses and individuals alike. A forerunner to GCS identified the struggle before cyber attacks became daily news headlines, and began strategizing on options for reversing the impact hackers and cyber criminals had already made on the nation's digital infrastructure. After extensive debate on the

myriad options for meeting their goal, they decided to embark on a secretive project to create a global cyber security surveillance tracking and data management system with much broader objectives than a single government had the time to imagine.

To accomplish this task, GCS moved directly into the U.S. government's fields of operation. As each federal government department released a paper or policy or draft legislation on a cyber security issue, a cadre of well-placed GCS operatives monitored developments to determine if a potential segment would have an impact on their clandestine project. Unofficial activities did not directly overlap official work, but functioned efficiently within the scope of government outreach. The group's covert participation emerged through a deliberate convergence of presentations at conferences as subject matter experts, fact-finding lunch meetings across government and business lines, requests for information from diligent journalists, and draft agendas developed by one-cause organizations and lobbyists. To the delight of the embedded outsiders, as the publicly offered details began to synthesize for more organizations and interests, one official government insider after another began unobtrusively asking if the time had come to strengthen the cyber security process by uniting across department lines and developing a more organized plan.

Two of those officials were Julia and Marco who were diligent undercover promoters of GCS's agenda. The group treasured the value the two emergent thinkers in areas of influence could bring to their operation, and lured them to the table with the promise of aligning with other objective-oriented achievers who had written their own success stories through hard-work and trained brains. As a businesswoman who started and ran her own investment firm, Julia was recognized for her strength and singular focus, as well as contacts in financial circles around the world. As a soldier trusted in military Intelligence, Marco was seen to have a loyal operational brain trained to protect American interests. GCS was not restrained in defining its mandate to the two rising stars. More specific than the imaginings of media and Internet conspiracy theories about an entitled establishment working outside the ropes of democracy, the group was strategic and productive in its intent to ensure its definition of economic survival. Members knew exactly how to operate when bounds were created by government and the populace, and how to re-arrange limits to adjust in their favor. The broader society outside their circle had no consideration in their activities. If others benefited from the accomplishment of their objectives, no credit was taken. And if not, no negative recognition was acknowledged.

Julia was tasked to spearhead GCS's goals with an international team of handpicked thinkers overseeing the research, creation and implementation of a detailed plan for the project, which when completed would be the physical infrastructure foundation for the surveillance and online tracking operations. In her assignment, she sought and expected to leave her lasting legacy entrenched in computer code. Civil liberties and privacy issues aside, she saw an opportunity to secure the future by committing to using technology to protect public safety on every level. To ensure the palpability of these ideas, she privately united other influential voices in national security, defense, business, academia and government to propose extending the system beyond surveillance to complete integration with individual online activity. The idea would encourage citizens to voluntarily attach to the system in exchange for a simplification of their everyday tasks. The win-win proposal gave citizens, efficiency and expediency, and governments, their information.

"I know the GCS agenda is intense but the project cannot be reliant on elected officials who change every four years," Julia stated as she uncomfortably shifted in her chair. She was shorter than an average woman but her statuesque voice made her sound much more commanding than

expected on sight. A scrapper from a violent inner city neighborhood, she had pounced on education as her ticket to upward mobility, and literally fought to be allowed to attend a magnet high school for industrious achievers. The Ivy League followed for her undergraduate and law school degrees, after which she joined the Foreign Service, before leaving to go into business. Invited back to run the State Department, she had served on the frontlines of the most dynamic changes rippling through the world. Not only was the West engaged in a thousand-year war with extremists, but also the rise of new wealth launched by China was changing the economic face and political influences of the world. Julia endeavored night and day to convince her colleagues that America's complacency and late 20th century view of global geo-politics would not hold against the challenges of 21st century realities. "We need to have a continuous multi-decade rollout plan adapting to changing technology and political events," she continued.

"I'm aware of our goals," Marco convincingly responded.

"Then why are you letting a reporter in to Horizon to snoop around and ask questions about an operation we have managed to keep secret from everyone?"

"I needed a safe place to look at her files. Horizon does not even exist on maps. The complex is camouflaged from satellite surveillance."

"You are taking her right into the building."

"In a blindfold, through underground parking, she'll have no idea where she is."

"And if she snoops around?"

"I think this one can be convinced to mind her own business in the name of national security."

"Really? Why?"

"She was my tenth grade science partner," Marco sheepishly replied.

"What? Who?"

"Dallas Winter at the National Republic."

"And you're still buddies?"

"Yes, in a manner of speaking."

"I know about Dallas Winter, she's one of this town's most relentless journalists. How deep does this friendship go?"

"Deep enough."

"Deep enough to keep her silent...a journalist of her caliber?"

"Yes, I think so."

"To make sure she does not learn any aspect of our operations?"

"Are you referring to a specific concern?"

"The money."

"The money?"

"We have finally earned the trust and confidence of those who will provide the money, and you're going to rattle them by letting a reporter into Horizon."

"No one will rattle them."

"We have worked more diligently on this part of the plan than any other, Marco. We needed to ensure the project had an independent source of funds to supplement unpredictable government resources. Investors, businesspeople, global financers, even Hollywood producers are agreeing to finance the project's experimental initiative in exchange for a seat at the decision table...the secret decision table."

Without governments to rely on for sufficient available on-demand funds, GCS had decided to cultivate permanent fundraisers, outside all government entities, to provide additional money

whenever the project ran short. The group's singular mandate was to ensure the system protected national security at all cyber and physical world levels. But other objectives, supported by broader business goals like obtaining real-time specific data on consumer activities, conveniently aligned within the same technical infrastructure and could be implemented as required on behalf of the financial backers. In exchange for connecting surveillance to consumer-facing online activities and making all of the data available for business analysis to further revenue and growth goals, the business community and private investors agreed to financially support GCS's project.

"We have to be able to ensure our money that the road ahead is clear, without the potential for fallout or blowback from wandering journalists," Julia stated.

"I can manage her. But when I convince her the files are not FedSec, she'll want to research more and show the documents to every other government department, not to mention all the think tanks in town."

"You think she's going to put those documents, with those titles, into wide circulation?"

"Not if we give her something in exchange."

"Like what?"

"The files literally are not FedSec. I'm not lying about my department's involvement, but I'll be concealing my knowledge of the actual origin. Because she might guess I know more, I want to give her the one thing every reporter wants."

"Oh I knew there would be a catch. What will she want?"

"The story."

"I hope you are not implying the typical meaning of that statement. This is not a story we can give."

"Not as we understand the details. But we can give her a piece, building on information the public already knows."

"Isn't Winter too smart to accept being handled?"

"Yes, but we will not handle her. She'll get a story, but we'll control the content."

"How will we manage her content?"

"She does not have all the files, at least I do not think she has. But she's received a preview. If we keep her information contained, we keep the story contained too."

"Contained how?"

"Look, everyone in the world is speculating about the future. There are stories every day about government ideas for regulating privacy or controlling civilian drones. I think she can be made to understand she's looking at proposals for piling into the debate."

"Are you sure?"

"Yes, why not? It's the most plausible explanation."

"Next to the truth."

"Well we both know she can never know the truth."

"But can she become a problem if she begins to suspect a bigger story. I mean, who are you going to claim created those policy papers, she'll still want a name."

"Okay we'll give her a name. One of those obscure European discussion meetings held every year in an alpine village."

"Seriously?"

"Why not? Maybe a low level government official attended and happened to use FedSec's template to create his discussion papers."

"No, do not mention FedSec or the government. She'll want the name of the official. I think you should deny any knowledge of the documents and the content."

"Really?"

"Yes, if she can recognize FedSec's template, another viewer could too, and recreate the framework for personal use. Having the template does not mean the document originated at FedSec."

"I'll have to take a look at how authentic the template really is. If the files are within our numbering sequence, someone could definitely notice."

"Sure go ahead check all the details, but do not let her believe you know anything about the content."

"And if she wants to keep digging?"

"Let her. She won't find the real story. In fact, she may do us a favor. However she tries to chase down leads, we can see if we have holes in our security or issues we have to deal with around guarding the facts. Leave the story as vague as possible, let her search and search, and we can follow and see how far she gets."

"I'm not sure I'm comfortable letting her run with her questions."

"Why? We kill two birds with one stone, make sure Winter does not get the story, while confirming our defenses are airtight."

"Are you sure you want to risk watching her investigative methods?"

"The other option is to have her arrested."

"For what? She's not dangerous or disloyal."

"Not yet. But if her snooping becomes a problem she could be arrested for asking the wrong questions and threatening national security."

"No, no way, let's not make allegations. I will keep her focused on a narrow range of issues. She'll never have the big picture or know the whole story."

"All right Marco, but this is all on you. You contain...and control her. Because if we see any hint the story is grow—"

"You won't. I'll make sure she stays silent."

"Good. I'll trust you to keep your word."

*

Alongside the Potomac River, tucked into the northwest corner of D.C., the exterior of the Horizon office complex appeared to be an established group of high-rises offering innocuous work locations for striving knowledge professionals. But inside, three of the four buildings were gutted as each floor housed only server stacks from floor to ceiling. The fourth building, where two agents escorted Dallas, accommodated functioning business offices on every floor. Dallas stared at the tightly dressed executives and polished assistants who nodded or politely said 'good afternoon' while passing by in the lobby. At automatic entry gates, the agents swiped biometric cards while cameras recorded their every move as they reached the elevator and rode to the 11th floor. Dallas was left alone in a stark office with a spectacular view of the river through floor to ceiling glass windows. Surrounding her were bookshelves containing a selection of business and technology bestsellers, but in the middle of the room stood an empty desk, devoid of paper, supplies, or even a small lamp. Dallas quickly calculated the office was not a permanent location for an occupied operational executive.

Sitting in a chair facing the desk, she took out her mobile and began checking messages. Several minutes later, she stood up to stand by the window and admire the view. Returning to her chair a few minutes later, she began idly surfing the Internet. After another forty minutes, when she was ready to cease debating whether to send a text to Marco, the office door opened and the director walked in. Dallas stood.

"Hello Dal," Marco said, smiling as he stretched out a hand to her to shake and offered no apology for his tardiness.

"Hello Mr. Director," Dallas answered accepting his greeting. Marco moved to sit at the desk. "I have to admit I was expecting a gray-walled windowless hole."

Marco laughed. "You watch too many movies, my friend."

"Well your approach was a little cloak-and-dagger."

"Comes with the job I'm afraid."

"Really?"

"Yes really. You know the era we are living in."

"You are concerned about terrorists?"

Marco laughed again. "Yes. But I was talking about D.C. politics and the media. You know every step we take is being scrutinized for a story to feed the 24-hour news cycle. This city is a fishbowl Dal, and I for one have to watch how much all those peering eyes are allowed to see."

"Okay sure. So how does this work?"

"Don't you have something for me?" Dallas reached inside her handbag and removed the flash drive. Without hesitating, she handed the device to Marco. "Hmm..." he suspiciously noted while accepting the drive, "...you've made a copy?"

"Why do you ask?"

"Because you made no demands and are not reluctant to give me your precious find. I assume you have a back-up."

"Well you did not expect me to just hand over evidence did you?"

"Yes I did."

"Why?"

Holding the drive up in front of his face, Marco hesitated then shrugged as he selected a button on the desk. "Let's see what you've got." Dallas jolted backwards when the desktop suddenly slid away like a panel, and a laptop computer rose up in its place. Marco grinned and motioned for her to sit down. Putting the drive into the laptop, he accessed the files and read in silence.

Dallas did not see his expression change or notice a sense of alarm. But his composure was expected. The FedSec Director would hardly be expected to cry with fear if a journalist picked up top-secret national security information. When Marco finished reading, he looked up. "Scary headlines and generalized content, you say this was left in a restaurant?"

"Yes, Infrared."

"Infrared? Cool place, hard to get a reservation there. Have you been?"

"Yes. You?"

"Yes."

Dallas waited another thirty seconds. "What are these documents, Marco?"

Marco leaned back in his chair. "As I suspected, an individual or organization's speculative policy thoughts."

"But the template led me straight to FedSec."

"What can I say? You know the schematic of a FedSec template, but so do hundreds of other people. Our instructions are not hard to copy."

"Marco, these documents contain specific information with detailed plans involving high-ranking people."

"Yes, people usually write policy ideas in a format that makes the content readily digestible

for government departments. People assume the government could implement the policy verbatim."

"And their assumption is not a problem?"

"Well depends on the administration, the policy, and the credentials of those who wrote the detailed implementation plan."

"You're saying the documents are not important, and I should what...search for another source?"

"No. Dal, there's no story here. What are you going to do, knock on every think tank's door and ask if someone lost a flash drive? I imagine such amateur behavior is beneath the talents of a journalist of your caliber."

"What do you recommend?"

"Well I know you like to follow your instincts. But why not ask the restaurant to put the drive in lost-and-found and wait until a customer picks it up. If someone was working hard on putting all the research together they'll want to claim their property before another idea wonk steals their opinions."

"Lost-and-found?"

"Yes."

"For documents professing racism and sexism may be coded into business and government websites? For policies about weaponizing civilian drones?" Marco stiffened. "You think these are lost-and-found ideas? Marco, I have never even heard of some of these plans. The one for replacing the entire public school system with computers is almost completely mapped out in detail, for every state."

"Washington is full of people who perform comprehensive research and planning, Dal. They live off the challenge. They want to be the first to tell the government they thought of all the possibilities, and the ones to hand the full story to the right members of Congress to discuss in committee. Details do not make the content real."

"These documents look real."

"Listen, I cannot spend all day discussing this with you. Either you believe me or you don't. But you're my friend Dal, so listen to a friend's warning. I highly recommend you do not publish these documents or any of the content or even repeat the names of the titles of the files. And I am specifically warning you not to make any reference to FedSec or FedSec's template or discussions with FedSec's director in connection with these files. Do you understand?"

Dallas stared at him, searching his face for a hint of leeway. "What are these files, Marco? I can tell you know more than you're saying."

"What files?"

"Marco."

"I do not know what you are talking about. The content on this drive is not FedSec documents. Do you understand?"

"Whose documents are on the drive?"

"I do not know."

"Yes you do."

"Do you want to accuse the director of FedSec of lying? If so, we will be walking down a different road, my friend."

"I'm not accusing you of anything."

"Good, now what are you going to do next?"

"What do you mean?"

"You know what I mean."

"I'm not sure what I'll do next."

"I'll give you some advice. I'm going to let you go without conditions, which one day you may discover is an extraordinary gesture on my part. You're going to go home and continue with your life. But I once again highly recommend you do not talk about the document contents or this meeting or anything at all connected to the last few hours from the time the drive was handed to you." Marco paused. "Actually who did hand you the drive?" Dallas did not respond. "Do you want to force us to find out?"

"What will you do?"

"Depends on the circumstances. Was the individual an unknowing citizen?"

"Yes, totally innocent. Some cleaning lady found the drive in Infrared and gave it to the restaurant's owner Fresno Tyler and he gave it to me."

"Why would he give you these documents?"

"Because he..." Dallas stopped. "Why do you want to know?"

"Why do you think?"

"Marco no," Dallas insisted, her voice rising in panic. "Frez has nothing to do with my investigation into these files."

"Did he give the drive to you because he read the contents?"

"Marco, no. His involvement is totally innocent. He has no idea what he saw."

"We'll be the judges of his knowledge."

"What do you mean?"

"We cannot have people claiming to have read FedSec documents when the material is not from FedSec."

"What are you going to do?"

"You do not need details. Focus on the advice I have given you. You do understand the advice I have given you, right?" Dallas wavered. "Seriously Dal, I am being kind and restrained right now. You understand, right? I do not have to repeat my advice and recommendations again, do I?"

"No."

"And you respect my advice, right? When I walk out of this room, I am assuming we are still good friends who appreciate each other's advice, yes?"

"Yes."

"Great." Marco stood. "The guys will give you a ride back to wherever you want to go. I'll see you around."

"Yeah, see you around." Dallas commented to Marco's back as he exited through the office door. She had no time to reconsider her world before the agents walked in to escort her out. The only action she had time to complete was to hit the 'stop record' button on her mobile.

*

A minute after Marco's escorts had dropped off Dallas at her home, her mobile phone rang.

"Yes," Dallas answered.

"Dallas Winter?" a voice asked.

"Yes?"

"You don't know me, but I know what you're doing."

"Look Frez, if this is some kind of joke," Dallas responded annoyed. "I've had a weird day. I do not need your crap."

"This is not your friend the restaurateur Fresno Tyler," the voice unemotionally responded.

Dallas froze. "Who is this?"

"You don't need to know my name, only my motives. I wanted to let you know you have guessed correctly. The flash drive you received last night is not a random think tank's policy paper." Dallas gripped her phone. "But the documents are not FedSec either. The content comes from a more influential source."

"What source?"

"I'm not talking about specifics, Ms. Winter. I'm only warning you. Stay away from the contents in those documents. The information is dangerous. There is a discussion going on right now in Washington...and London, Paris, Brussels, even Beijing and Moscow, and believe me, the words and policy ideas in those conversations transcend top secret."

"You really expect me to believe you? Who is this?"

"I know you recorded your conversation with FedSec Director Manuel." Dallas was stunned into silence. "When FedSec vets an electronic device they put the controls on their own internal monitoring system. They know you were recording too. Don't even think you can use the audio. But if you try to broadcast the conversation, they'll erase the file, unless I get to your laptop first."

"What the fu—"

"Dallas, believe me I'm a friend. I'm helping you. Don't provoke people about those documents."

"Who is provoked? Who are you?"

"My name is Apex. And when I say I'm a friend, I'm being truthful. But let us handle the issues, stay out of this business with the 2100 policy files, okay."

"You have got to be kidding..."

"You have been warned. Don't push your luck Dallas, and do not follow up on this story again." Before Dallas could re-express her anger, Apex disconnected.

*

"You let her know there was something to fear?" Julia chided Marco. "You left a journalist thinking there's a story in those files?" The fading evening peered through the window of Marco's Horizon office where, on his laptop, he had paused his replay of his recorded conversation with Dallas.

"She won't make a move," he told Julia who faced him across his desk with unshielded anger.

"What makes you so certain?"

"She has no usable information. A flash drive with a bunch of documents appearing to be thought pieces is hardly verifiable evidence. There's no story and speculation would be ridiculous. If she makes an accusation, we deny her version and she looks like an idiot."

"Except her statements would not be speculation, but the truth. The contents of those documents are the real plans of the government of the United States."

"Not even the government of the United States knows those documents are its plans."

"She has information we cannot let spread."

"She won't say a word. I've shut her down, and the restaurant guy too."

"What did you do with him?"

"We double-checked he had not read the files and had no interest in the story."

"How did you verify his interest?"

"We went through his recent communications, from the time they found the drive."

"And?"

"Nothing. He's not talking to anyone. He's okay."

"Are you sure?"

"Positive."

"I hope so. You realize we are in the best situation we could ever be in for the plans we want to execute. Our timing for this project is serendipitously beautiful. The complete dysfunction of Washington politics has been a blessing for the entire scope of our objectives since day one. We could not have asked for a more perfect point in history for launching our work, but with this reporter...we are facing a disruption."

"Dallas will not be a disruption."

"Obtaining formal bi-partisan approval for our project would have been impossible. No one in Congress is approving major projects on the record. Legislators want to avoid demonstrating cooperation with the other party. Informally we can do as we please, no one is watching. The two parties do not speak to each other. Every member of Congress is looking to secure an individual future regardless of the impact a lack of action is having on the country, which means we can select the most effective operators to open doors where needed. Money is running wild while there is no tax reform or campaign financing controls, and no targeted spending on important initiatives. We can take bits and pieces from various sources and no one notices. The gap between the federal bureaucracy and elected officials could not be wider, leaving us a great yawning hole to manage to our benefit. We can send instructions to a federal civil servant and receive instant results because, with a lack of leadership, those poor people do not know any better. If we actually had to manage with a hard-working, committed, functioning government, we would never have been able to implement our project."

"Yes the circumstances are perfect."

"And you want to destroy our convenient alignment of inept behavior for your friend?"

Marco stared at her. "No, of course not. If Dallas chooses to speculate on the origin of the documents, the story cannot be corroborated. No government department or agency is officially implementing the project. As you said, the current lack of cooperation in government means most of the contributors to the research had no idea why they were asked the questions they were asked about cyber security or the intention of the information gathering."

"But every government department and agency will be unofficially made to accept implementation of the project, if they want to or not. And only about two dozen people around the world know why. And those people are expected to keep the secret for the rest of their lives. Your reporter is not committed to our secret, but she has our information."

"Yes I know. But she's contained. She does not know the context for the information. Tell me your real concern."

"I want a comprehensive idea of where we are on each subject area. If she starts talking, we need to be able to deflect attention away from activities in the real world that are preparation for our activities in the...future world."

"What do you mean?"

"Well let's take the discrimination file. Can she learn about our future plans from activities we are conducting in the real world?"

"On that topic, no. Race and gender politics are rising to a crescendo we have not seen since the '60s and '70s. Back then there was no expectation of equality, people were protesting for basic rights. But at this point, expectations are sky high and so are the disappointments."

"Don't remind me."

"Hey, you're a woman Secretary of State."

"One high profile cabinet post. Where's the woman Treasury Secretary or Secretary of Defense? The Senate should be a minimum of 51 women, and the Supreme Court a minimum of five woman justices."

"Okay, okay, you can't have everything."

"We are the majority, more than fifty percent of the population, and we have no power."

"Right."

"And don't get me started on ethnicity. Sixty million Latinos in America and you barely have a place at the Cabinet table."

"Yes I know."

"Every forward step of the civil rights movement is being repealed and pummeled back into history."

"Because the middle class had its heart ripped out by the housing crisis and they need someone to blame."

"The politicians use simplistic, narrow solutions because they are all too lazy and stupid to work on real issues for turning around the economy and education. They pick an emotional target like voting rights and stomp all over the issue instead of launching a major initiative to find effective answers for creating jobs."

"Okay, okay, where does the current social status put us with the data Dallas uncovered?"

"The discrimination file essentially warns the software code governing today's consumer facing websites can be made to respond to an individual or organization's sexist and racist policies, or even innocent stereotypes, and no one will ever know."

"If a business does not want a particular demographic to obtain its product or service..."

"Or they want to charge certain people more..."

"The software will let an organization seamlessly implement those policies. All they'll need is access to demographic data. Sites requiring people to post a picture will automatically have identity information, if they have the software to decipher the picture's content. Other sites will have people enter the data in the name of benign statistics gathering. And others will access the data from other websites or databases feeding information to businesses, for a price."

"There's also name and location politics. The applications can be made to interpret where people live or the name they give, as an indicator of ethnicity or economic status."

"And they can proactively alter the code or innocently make changes based on programming existing stereotypes into common questions."

"There's nothing innocent about stereotypes."

"Right, but the question is...in terms of our project, do we care? The result of online discrimination will hurt people on an individual level, but is the outcome going to be the kind of problem that halts our other plans?"

"Technically, there is really no reason to care, the issue is almost impossible to prove."

"As a person I care."

"But as the director of FedSec?"

Marco hesitated before unenthusiastically replying, "No."

"Believe me, as a woman I care too. I know turning the other way is tough, Marco. But somehow we'll have to transcend this technical functionality. We'll have to find another road to our power and economic security."

"There is no other road. Women are already far behind in tech employment and that's where the money is. If you get left even further behind by male-run online companies unrepresentatively programming your access to products, including education by the way, you're

going to completely miss out."

"But we need our cyber project. If we do not gain total control of our domestic security, the country could become impossible to live in. We could have bombings and mass shootings every day."

"Yes I know. The general idea behind our entire plan is surveillance. If we can monitor public places, have dynamic facial and body recognition and automatic alerts for suspicious behavior, we can finally get ahead of the terrorists."

"I don't think the average American is really going to cry about the price they're paying, most of them are already enwrapped with their mobiles. We are talking about a population barely looking up as they go through their day. People have no idea how often they are viewed on camera."

"I know. Indifference is one development I have never reconciled. When did people become so complacent?"

"The 2008 recession sucked the dynamism out of the general populace. The crushing of the American dream of home ownership really prompted a lot of people to give up. They thought they had done everything right, but a configuration of indecipherable financial equations destroyed their hard work over night. People lost all their equity, every cent they had ever saved. Do you think they are going to turn around and start working hard all over again? Not if they can avoid the pressure."

"Yeah I think the true social fallout from 2008 has yet to be written. But the effects are being played out in everyday life. The rise of smartphones came just in time to provide people with a distraction from ever making an effort again. With the malaise, people were waiting for an opportunity when they would not have to struggle. Now they have found one. Without a depression or a war to recover from or an evil dictator to be afraid of, people can settle into their docile lives without guilt. Staring at your mobile all day is not a sign of laziness, in fact most people would assume you were engaged with someone."

"That's the irony. Most people are not using the smartphone to do anything smart. They are scrolling through social media updates."

"Which means they'll barely notice when our system comes online, and we track and store their every move."

"No, they'll walk right into the process."

"With their heads down." Both laughed. "But we begin a high tech race and gender war at the same time?"

"Only with those who are paying attention."

"The issue is indirect. You can no longer hang a 'whites only' sign in front of your business, but you can code the directive into your business software. Since consumer websites are already collecting demographic data about people, as the information becomes cross-referenced and traded, every business will eventually know each individual's ethnicity and gender, and react as they wish."

"A cyber Jim Crow world."

"Exactly and no one would be the wiser. Complainers will have a hard time proving the computer rejected an applicant or buyer because decisions are made in split-seconds with no face-to-face interaction."

"Without transparent standards for gathering and using personal data, you could also weed out people by education, profession, or location."

"Right, you can have the system automatically reject graduates of a certain college who

apply for a job. Or you can have a 'no journalists' policy at your hotel. A person whose profession is cross-referenced as journalist will always receive a 'there are no rooms available message' when they try to make a reservation at a hotel."

"And a second later, I could book a room because really the hotel is only at fifty percent occupancy."

"That's the idea."

"Yikes."

"And the possibilities go on."

"Actually given those scenarios, maybe the outcome could also go the other way. Once these discriminatory practices start affecting white people...and men, the media will pay attention. Tech companies might have to think of ways to use software to fight discrimination."

"How?"

"I don't know. But everyone will know they can track the discrimination decisions. They will know when a woman applicant is rejected and a man is accepted. Every company would have statistics."

"But they could also manipulate and manually change those numbers at any time. You would have to be able to infiltrate the business' systems to monitor activity 24/7."

"Well there's a job for the hackers. Besides directly stealing consumer data like credit card numbers, businesses will have to watch out for hackers who practice data analysis on their decision-making information and publish those statistics to the public."

"Yes maybe some hackers are civil rights activists or working with them. Imagine those stories. If a business is suspected of having coded discriminatory practices into its software, hackers could access those systems and pull the data before the business decides to delete or manipulate the findings. The ability to analyze those numbers would be a game changer."

"Hackers would need to get organized if they are going to become the champions of civil rights. Businesses would instantly fight back, the data would be considered stolen. The hackers would have to have documented evidence they could prove, which would not be easy. They too could be accused of altering the data."

"You would need cyber forensic scientists on top of cyber forensic scientists to investigate for the manipulation of the code."

"Absolutely."

"We are dealing with a real, but distant, possibility. Not only are those hacker guys...mostly guys, super-competitive, but they are also all over the world, and by definition, independent."

"You would need one who saw this coming and started mobilizing forces right away."

"Yes if any of them are even aware of our plans, his work is set, and he should be preparing a response right now."

*

Apex repositioned her back against a tree in a park across the street from the Horizon building, and tried her access program again. After the fourth timeout message, she cursed the limitations of mobile technology, and began slowly walking back towards the shopping mall parking lot where she had left her car. Her phone buzzed. Glancing at the displayed name, she stated, "finally" as she answered.

"You shouldn't keep calling me," Carter Harden, the founder, president and CEO of technology industry giant Initium immediately chastised her.

"We have a problem."

"You have to deal with problems. You know I can't, I run a public company."

"Don't be so rude. If you want to keep running your precious company you'll listen to me."

Carter took a deep breath. "Okay?"

"Dallas Winter."

"Who?"

"Dallas Winter, the journalist who picked up the files."

"And?"

"I don't think she easily scares."

"Find another way to intimidate her."

"She knows she has a story because your buddy Marco Manuel basically told her she had correctly guessed the source for the files."

"You've got to be kidding me?" Carter looked up and rolled his eyes. "How do you know?"

"She recorded the conversation and I had a listen. I'll send the file to you. Manuel did not directly tell her, but he's also not very good at denial."

"But why would he give up the information?"

"They're old friends and he thinks he can control her."

"Seriously? Okay, any guesses on her next move?"

"Nothing yet, but who knows what's she's thinking. I have not yet developed mind-reading applications."

"Too bad, you'll have to pursue her the old-fashioned way. Be a stalker."

"Fun. And how are you going to handle your friends?"

"I'll see if I can rein in those Washington dopes. Like I need more complications. Stock is flat-lining, I've got a thousand interview requests, and I have to deal with incompetents who do not understand a straight-forward mandate to implement the technology foundation for the next hundred years."

"Not everyone has your cold calculating brainpower, some people care about their friends."

"Their friends will get us killed, literally and figuratively. If the press learns of our plans the publicity will set us back decades."

"But my work will be done."

"No, your work will re-double. The U.S. is going to go forward with an integrated surveillance system in one form or another. The idea is too tempting. Imagine the ability to not only track every single human being on earth, but also to use the information gathered about them to provide daily life instructions tied directly to government and business objectives. Most people are complacent, risk-averse and followers. The idea would work perfectly if the project were fully rolled out. Your work will not end because you will have to stay on top of governments and make sure the system never comes online."

"You have to make sure too. You're the guy with the technology they need."

"They'll never fully get my technology...my real capabilities. They might not understand that right now, but I'm not giving up my brainpower to governments."

"They still believe you're one of them?"

"Yes, of course. And believe me, a lot of guys like me will align with them. Most guys will not be able to resist those lucrative government contracts."

"The work goes on regardless of the information Winter is able to uncover?"

"Absolutely. We have a duty to humankind to prevent this project, we have to stick to our objectives."

"Okay I'll follow Winter and let you know if I learn anything."

"Good, let's see if she can't be the catalyst that forces FedSec to reveal its weaknesses."

*

Under conventional circumstances, Dallas would consider two straight days of permitted direct access to Marco Manuel to be the beginning of the apocalypse. Not only was he willing to see her again, but he also seemed enthusiastic about her request, as if a sudden realization had come over him. Fitfully, to her surprise the contentment was shrouded in mystery as he insisted on her being taken once again to his private office at Horizon. Twenty minutes prior to arrival, Dallas was blindfolded. After emerging from the building's underground parking structure into the public areas, she had little time to view her surroundings. The extreme northwest corner angle of the capital's diamond-shaped geographic layout was a sedate neighborhood of riverfront parks backing into Bethesda, Maryland. As Dallas looked through the lobby's glass entryway, she latently realized the location should have been a revelation. 'Why does FedSec have offices in a semi-residential nature zone?' No answer would be forthcoming as Marco's earlier friendly demeanor turned to soured concern.

"You have an emergency?" Marco abruptly stated as she entered and sat down on the other side of his desk.

"Yes, I think I do," Dallas responded, defending her appearance. "I received what I can only consider to be a threatening phone call about those files."

"What files?"

Dallas sighed. "Okay about the flash drive I spoke to you about yesterday."

"What kind of threat?"

"The 'stay away or you'll have trouble' kind."

Marco raised his eyebrows and asked with genuine concern, "Any idea who threatened you?"

"A woman. Said her name was Apex."

"Apex? How original."

"She knew where I'd been meeting, who I'd been meeting with. The conversation was very scary."

"What do you mean 'where' you'd been meeting?"

"She knew I had a meeting with you."

"Oh. Did you recognize her voice?"

"No."

"Did you see anyone following you?"

"No."

"Any other clues?"

"She said the files are part of a big discussion in London, Paris, Beijing." Marco imperceptibly braced in his chair but did not display any concern. "What do you think?"

"You've been frightened by a crackpot."

"Who knew how to find me and private details about my activities?"

"That's a price we pay in today's world. No doubt you have plenty of private information already available online."

"Hardly."

"No public pictures of you with your friends?"

"Well sure but—"

"Posts about conferences you went to, photos of trips you have taken?"

"Work yes, someone else's pictures, but personal no."

"Only a couple of public data points are necessary and they've got you."

"You think some random person has come along and found me, identified me, and knows I have the files? Does this person monitor surveillance cameras too? Because otherwise how would she know the drive was found at Infrared and given to me by Frez Tyler. Why are you so sure that could be possible? What is this really all about, Marco? What exactly was I handed?"

"Did I not warn you about discussing this—"

"You said don't discuss the content in the files. But now I'm being threatened, and a personal attack is another story."

"You're okay. I'm sure she was playing out some kind of prank."

"Marco, are you really going to leave me vulnerable to someone who had the technology to track me down so specifically?"

"I don't think you are under threat from any—" Marco stopped to stare at his computer screen. Prior to Dallas's arrival, he had activated his laptop to emerge onto the top of the desk, and the screen had been statically on during their conversation. But as Dallas was speaking, the background image on Marco's monitor suddenly became overlain with a message he had not entered. "What the—"

"What is it?" Dallas asked as she stood to walk towards him.

"No!" Marco shouted stretching out his hand to stop her from advancing and seeing the screen. He hit a button on his desk phone and summoned security. When two men appeared, he said, "Escort Miss Winter home." The men nodded but Dallas did not move. "You're leaving now," Marco said, noting her reluctance.

"What happened? Tell me?"

"Go voluntarily or we'll force you out."

Dallas glanced at the guards and back at Marco. "Just tell me."

"Take her out," he ordered the two men. The guards grabbed Dallas's arms and dragged her out while her voice pleaded with Marco to explain.

When Dallas was clear of the door, Marco instituted a security alert for his office and summoned his deputy at Horizon. "Has anyone reported an issue with our systems?" he demanded when the deputy entered.

"No, nothing," the deputy insisted. "With our firewall? No one can get in here."

At his words, Marco looked again at his laptop and glimpsed the USB drive Dallas had given him laying in a tray inside his desk cover. He picked up the plastic device. 'No one has managed to get in unless brought in,' he silently cursed. Marco's computer had an automatic scan for viruses on external storage devices, but a clever tech could overcome the standard process if the files on the drive were made to display, inside and out, internal FedSec protocols. "Okay thanks, out," he said to the deputy, who immediately left. "Shit," he exclaimed as he contacted his personal tech support to come and collect his laptop. Immediately afterwards he phoned the Secretary of State to confess that evidence of the 2100 policy files were now likely in the hands of an unknown cyber enemy. While he waited for Julia to connect, he stared at the glow emanating from his laptop monitor where the sight now displayed before him on the screen was quite decisively the words, 'Thank you.'

*

CHAPTER TWO - THE EDUCATION FILE

In a Washington, D.C. cafe where interior noise was overwhelmed by water flowing through a monument on a nearby plaza, Apex scrolled through FedSec's detailed blueprint for a domestic cyber security interlocking surveillance system, nicknamed COSA for Complete Online and Surveillance Aggregation. COSA, as far as she could tell, would connect all of the ground surveillance cameras in the country with overhead satellite coverage from outer space, and strategically placed material and body sensors, to track everyone operating in public spaces. To bolster law enforcement's opportunities to catch terrorists on domestic soil before they acted, the Commission was implementing an extensive research initiative to determine how to co-opt every camera already recording on street corners, at intersections and inside public buildings. The next phase would ensure dedicated law enforcement satellites and an army of security drones ready to be directed at any time to focus on specific locations where terrorists, criminals and suspects may be operating. But the ability to view people in the open had to be aligned with a protocol to separately determine the identity of each individual. To achieve that goal, the system would need advanced facial recognition software capable of scanning across databases to match features to known records. But since appearances could be precisely altered, the system also necessitated functions to understand physical body size and shape, movements and gestures, and the capability to decipher clothing and accessories a person was wearing or carrying by cross-referencing personal items to individual shopping records. In the future, the report read, if the system was unable to make a facial or body match, the software would advance to analyzing the person's clothes, determine the color and brand, cross-reference across all purchases of the same product and find a consumer match to the suspect in retail website databases. The idea, claimed FedSec, was to prevent an individual from completely evading the system's ability to utilize surveillance footage for identification and apprehension by wearing hats or dark glasses, or continuously keeping his head down to prevent his face from appearing on camera.

After finishing with the detailed plan, Apex began reading a series of documents from various federal government departments indirectly supporting the project. The Attorney General's office had added an analysis of the legal implications of the functionality, which according to Justice Department researchers, were limited. The country's lawmakers declared the Constitution did not protect an individual operating in a public space from being observed and recorded, because there was no expectation of privacy. Law enforcement was not prevented from using surveillance in a non-invasive fashion against the populace, and later using the evidence of the activities to make a case against an individual who had committed a crime. The only issue would be the advanced science and technology aimed at confirming identity without a facial match. Could the system really determine a person's distinct form of walking down the street? How would the courts interpret a computer's analysis of swagger? Supporters argued the research would address those issues. But detractors noted civil liberties groups would find holes in the entire process. What if someone was ill on the surveillance day or on crutches or had a sore arm? How could the system know every oddity in a person's movements? With the conflicting opinions, DOJ declined to speculate on all of the arguments, but was prepared to begin research immediately.

In a response memo, COSA's sponsors already had an answer for those concerns. Since every aspect of an individual's life would eventually be linked to COSA. If a suspect identified through body movements were on crutches, the data would cross-reference the suspect's medical records and determine if the excuse was valid or advise of the possibility of an incorrect match in the analysis. Apex indignantly shook her head at the depth of the planned invasion into people's personal records and switched to reading the State Department's report.

State had been asked to assess the international receptivity for a global system rollout. Who among the U.S.'s allies would be most willing to finance and construct the same surveillance protocol and link their visual coverage to the U.S.? The system will be at its zenith, FedSec proclaimed, when every inch of the earth was under surveillance and every human had a profile in the system. The global view would isolate any suspect's whereabouts worldwide.

The document laid out several hypothetical case studies for combatting home grown terrorism, including one scenario about a child born in Minnesota who upon the issuance of his birth certificate, would be immediately registered in COSA. Throughout the child's life the system updates when he gets his inoculations, begins school, signs up to play football, takes his first job making burgers, buys his first car, submits a college application, and hands in an employment application to an operating business. His online access by phone, laptop and other devices would create the overall picture of his friends, habits and even word use preferences. Specific access numbers tied to his credit cards, health insurance, college debt, public transit use, travel and shopping habits would be aggregated into his record. The system would continuously scan for activity and ignore those law-abiding citizens who were also functioning as predicted through a standard life plan. But if after the first year of college, the now grown man's activities ceased appearing in the data records, the system could send law enforcement an alert. COSA's algorithms would have to account for out-of-country vacations and use additional tools to cross-reference credit card purchases for airline tickets or hotels stays and restaurant dining in other locations with the same timeframe as the missing activity. But if the search indicated the man had no results for thirty days, a warning could be distributed worldwide. Law enforcement could interpret a missing individual to be a victim, or a suspect who may have disappeared into a clandestine life. If he suddenly re-appeared without explanation, his actions would almost certainly be considered suspicious.

On these scenarios, the Justice Department had more to say. All consumer-facing services would have to rewrite disclaimers to provide transparency about third party uses of the consumer's data. Supporters warned such revelations would undoubtedly lead to a proliferation of service providers who would guarantee privacy for a premium price. Here the government would have a class war challenge. If wealthy individuals were able to buy their way out of COSA, not only would law enforcement miss potential suspects, but also the middle class and economically disadvantaged could launch a revolt. Many cautions were required to make the system palpable to the widest range of people. The government would need to ensure everyone had a profile, regardless of wealth. But to achieve maximum utilization, the government would have to implement standard opt-in protocols before the wealthy could determine how to avoid being covered.

Apex laughed at their naivety. Little did the official researchers know how far behind the government had already fallen on this point. People with money were the primary backers of independent technologists with plans to counteract government initiatives aimed at monitoring online activity. But reading on, she understood how COSA intended to inculcate everyone through the Internet and mobile phones. Utilizing a publically available service would automatically create a profile for anyone not already registered in COSA. The data collected through random use would be transformed into permanent files capable of creating commands for the individual user. 'To avoid this outcome, the rich will have to create their own internet too,' Apex thought. 'More work for me.'

Continuing to read the blueprint for a multi-year research and development strategy, Apex realized COSA would be slowly created by interlocking existing hardware into one controlled

system. The server farms currently established in isolated corners near rushing rivers or in hidden valleys in quiet towns would be brought together under COSA's control. The Commerce department's contribution to the report warned the government would need to provide an incentive to businesses to integrate with the system, but not legislation, which would be too public and viewed as draconian. Instead, the department suggested the output of the dedicated research required to create the system should be shared with businesses from the beginning. The government could allow citizen profiles to be accessible by public companies to use for marketing and tailoring products directly to people based on the details collected about their actual habits. The incentive to business would be the ability to know the exact products and services the populace is purchasing, how much they are spending, and the analysis of trends to predict future consumer activity based on searches and queries. The government would ensure the research included extensive inquiry protocols for consumer-facing industries. In exchange, industry would be expected to cooperate by attaching their server infrastructure to the domestic, and eventually international system. Law enforcement predicted that as the system proved its value by catching terrorists and reducing crime at home, more businesses would be incentivized to voluntarily link to the process.

'What a beautiful plan,' Apex sarcastically concluded as she nearly slammed down her computer screen. 'Too bad, it's doomed.' In the near past, when governments sought to mobilize against their own citizens, the rulers would call up a physical army and order the soldiers to attack the people in the name of the particular stand being taken. But for this mobilization, the people would be able to fight back with their own army, one they did not recruit nor see, but one standing up for their rights and fighting around their powerlessness. As the government began its movement towards solidifying COSA, Apex and independent technologists like her would rise from the public and private ranks to enforce a rational accounting through their technical capabilities. Her colleagues were having their own meetings and making independent plans to stop COSA before the system could be implemented. Their number one weapon would be advanced technology, including the brainpower to 'outcode' government operatives. The only question was when, and where should they start to deploy.

*

"An errant flash drive?" Julia questioned Marco in a gray-walled windowless room. "The whole incident was a set-up from the beginning?"

"It's possible," Marco replied leaning back into a sofa and putting his feet up on the table in front of him. They had retreated to the basement of FedSec's main office building where secure rooms with recording devices and video cameras were available for discussion of classified topics. A clock on the wall displayed the time as 1:10 am. Marco had entered the facility minutes earlier to personally access the room's operations and shut down the listening and viewing recorders for their conversation. "We need a new place to work."

"Impossible to move at this point. Besides the issue is not the building, the attack was against our servers and software. We'll have to fix Horizon."

"Fix Horizon? Some hacker could have lined the server rooms with damaging code aimed not only at listening to us but also stealing every file we have. He probably already has every file we have."

"You think we are too far along with the build-out at Horizon to take another course of action?"

"With our plans?"

"Yes."

"Well we would have to stick with the main concepts, the core structure we had decided on is definitely far enough along. But the details, no."

"Hmm, don't you think a hacker only wants the details? Wouldn't they already be suspicious we were working on global surveillance tracking? Conspiracy theories often have a way of actually being true."

"He may have been suspicious, but now the rumors have been confirmed."

"That's okay, as long as our enemies do not have the details. We can change the specifics and throw off the advantage they thought they had obtained by stealing from us."

"I don't know. How differently can you code a program to do the surveillance work we expect?"

"Coding is not my area of expertise. But we can have our Silicon Valley friend take a look for us, and let us know if we are okay to move forward or if we have to start again. He could also check the physical Horizon infrastructure and confirm if we really have to worry about moving."

"If you are speaking about the friend I think you are speaking about, contacting him would be extremely risky. He said we should only reach out in a genuine emergency. People cannot know his connection to us and to this program."

"We have an emergency. A hacker has infiltrated Horizon and possibly stolen all of the Horizon files. Our plans are in jeopardy. You have quality people working on a possible breach, but you do not have the depth of technological prowess our friend can access. He has a team capable of conducting a much more thorough search than your analysts to uncover if we are truly at risk."

"Maybe we are better off not playing that card right now. We can fix a potential breach ourselves. If this situation becomes volatile, we are going to need our friend in the future. I do not want to cry wolf."

"We are not crying wolf. We already know the system has been attacked. What are you really afraid of?"

"Being hasty."

"Or being exposed for having made a mistake?"

"What are you talking about?"

"You took a flash drive from a reporter and put an access file directly into Horizon's system."

"Be careful with the words you are using, Julia."

"I'm only wondering if the real reason you are reluctant to contact our friend is because you have more to hide than an innocent mistake."

Marco slowly lifted his feet off the table and deliberately placed them on the floor as he moved to sit up straight. "Are you accusing me of irresponsible behavior?"

"No."

"What are you attempting to say with your statements?"

"Marco, I'm not your enemy and I'm not accusing you of any wrongdoing. But we are in a dangerous place. Our activity is not public information for a reason. We are not interested in having the public learn about our plans because the public may not appreciate our intentions. We are also being forced to establish a plan no future administration could disrupt. You and I will not be around to see COSA through to fruition. We will be replaced and we will die, but the system will carry on. We have to make sure we do not disrupt the ability of this project to live on after we are gone, and the only way to do that is to ensure the foundation is established today.

Dallas Winter is a friend of yours, but you and I no longer have friends on the outside. We gave up our 'regular world' connections to ensure our nation's long-term security. The damage has already been done, very few names are connected to COSA, but two of them are ours. Under no circumstances can our positions be revealed, nor anyone learn the details of the operation. COSA will function autonomously. Future administrations will not be able to dismantle the legacy we have built, and more importantly, they will not want to. We are constructing a functioning, automatic process designed to stand-alone forever. We cannot make mistakes."

"I'm well aware of the stakes. I know the future we are building. I have been a champion of this plan from the beginning."

"We are hardly the beginning, Marco. Many minds before us set out on this path."

"Yes I know. But we have carried their ideas further than anyone. Like you said, COSA has to operate autonomously. We are the first administrators to solidify the reach of our intentions because we have identified the money. Once this project is financed as we have proposed, the rollout can continue without interference from levels of government. The real beginning is now."

Julia sighed. "If you believe that then there's even more reason to be vigilant. We are moving forward, there is no room to turn back." She stood and walked towards him. Sitting, she took his hand. "I did not mean to sound like I was accusing you of being negligent. But I think we, all of us, have to discuss how we are going to protect the operation we have built. We are going forward with this program, total surveillance is the best option for our country, for the world. Imagine an online file for every human on earth, immediately accessible to match suspects before there is an incident. We can bring terrorism to its knees. That's the goal here Marco, the end of living in fear."

"I agree and I swear to you I know my responsibilities to our project."

"I know you do. But we have to call our friend. We should be totally transparent and prepared to establish our own internal security protocol for moving forward together. We need to talk to him."

Marco dropped his head and stared at the floor. "I agree. But I want to be clear." He looked up at Julia, his eyes rimmed with defiance. "Dallas does not know anything. She saw a bunch of unidentified policy papers, nothing more. She does not know about COSA or programs connected to the broader project implementation."

"I'm sure you're correct, but Dallas Winter is not the disrupter I'm worried about."

"You want to find out who the hacker is?"

"Of course. But not only who. We need to uncover the information this hacker took from Horizon, and the plans he has for the evidence he found."

*

On a white, laminated dry-erase wall, a schematic separated various scenarios with dense red lines. Each predicted alternate versions of the initial rollout of COSA over the next ten years. Under one column, the rollout would connect every single surveillance camera in the country. The camera's feed would upload directly to the COSA database, 24 hours a day. The government was preparing to encourage every jurisdiction, business, school, and public place to voluntarily insert a wireless transmitter into each camera to send images to a local server farm connected to COSA. Or alternatively, legislation could be introduced to ensure surveillance cameras sold or used in the U.S. were pre-equipped with technology designed to automatically turn on the transmitter when the camera was connected. 'That approach would capture consumer surveillance cameras at people's homes,' Apex thought. 'I wonder what the public would think of

that.' As she considered another column, she heard a faint knock on the door.

Her apartment was located in a non-descript low-rise a few blocks from the columned 18th century buildings on the postcard-perfect campus of the University of Maryland in College Park. Living within a catchment area for 38,000 students, Apex accessed project supplies, computer hardware, coffee and pizza, with little notice. Diverse college towns were favored residential locations for independent technologists. The bustling attraction of a multi-hued populace wearing all manner of clothing from business suits to shorts and flip-flops; with hair styles capable of catching in tree branches or cropped to qualify for military service; and food ranging from extracted anti-allergy air to stuffed rolled animal-style animals, provided a background upon which any free human could throw a tapestry of pursuits and engage with many or remain alone. Less than nine miles from downtown D.C., the town provided Apex with her safe haven away from a location where everyone was considered suspicious.

Opening the door she smiled in surprise. "You are here," Apex greeted her visitor as she moved aside to let him in.

Carter Harden stepped into the apartment with the straight-backed intention reflecting his multi-billion dollar net worth. "Well, sounded like you were nervous," Carter responded with a smile. "And I don't like when my favorite people get scared."

Apex stepped towards him, took his face in her hands and kissed him full on the lips. "Or your wife," she commented, returning his smile.

He kissed her back. "Or my wife," he agreed. "What's going on?" Carter demanded as he moved further into the room and walked towards the couch as if he had just come home from his workday. Apex glanced at him with uncontrolled admiration.

Carter had been born to a single mother who never left her father's wheat farm near Minot, North Dakota. The family's daily meals were derived mostly from their own production and any extra purchased with money earned from sporadic outside work. Attending all of his local schools, working at service industry jobs, and tinkering with computer code were the only activities permitted to Carter. But the constraint of low expectations was not accessible to his DNA. Six months after graduating from high school, he decided the thoughts in his brain trying to determine how to attend college, start his own business and operate with thinking people, were not useless dreams as everyone around him preferred to proclaim. Knowing if he did not leave his insular prairie town, he was in danger of succumbing to its beer drinking, beaten down shooting Sundays, he packed a backpack, walked through the winter snow to the Greyhound bus station, and boarded the first connection heading west towards California.

Settling around Palo Alto near Stanford University, he found a bed to rent in a house full of computer science students, and took two jobs serving burgers and fries during the day and mopping floors at night. In his spare time, Carter challenged his roommates over their homework until one of the students dragged him to see a professor who tested him, marveled at his scores, and worked with admissions to allow him to enroll in classes on a work-study scholarship. From inside a classroom, surrounded for the first time in his life with like-minded equals who thrived on a life of intellectual achievement, Carter vowed to finish his education before embarking on a business career. But when he awoke in the middle of the night thinking of program code for a computer game that doubled as a type of synthesizer to aid with college-reading assignments, he rearranged his plans.

Within two years of arriving in the west, he was a millionaire. Still vowing to finish college, over the next ten years he created four more companies, and a day after his most recent public offering, he graduated. The next day, he created his own venture capital firm and declared his

intention to invest the money in determined individuals with insuppressible ideas.

One day during his business building years, Carter had gone to visit the professor who had helped him enroll at Stanford, and discovered another student already in his office. The woman, dressed in jeans and a t-shirt, looked to Carter's eyes as if she too had come off a farm, although as he was later to discover, disguise was one of her qualities. Her name, she claimed, was Apex. A day later, in bed, they talked about the companies they intended to build and their shared interest in cultivating technology developments for advancing the world and pushing humanity forward. "The dream of my life has always included finding people who are on my wavelength, ready to work and contribute as I am," Apex had told him. "I'm so glad you are real, so happy my vision is possible."

Carter's contented grin matched her satisfied realization. "More than possible," he said. "Your vision is happening right now." After her graduation, they privately married, bought a house in San Francisco's desirable Pacific Heights neighborhood, and focused on their businesses. But as Internet companies began to rise in economic, social and cultural dominance, Apex became increasingly concerned about the co-opting of technology companies' consumer data by the government's national security agenda. With controversial legislation to support their demands, law enforcement had determined the data contained in private companies' servers was fair game in a criminal investigation, even though the companies had promised consumers to keep their data private. The battle was one-sided so far, with the tech companies forced to cooperate or be branded traitors bent on aiding terrorists. In the government's actions, Apex saw two equally disconcerting developments. A law enforcement process avoiding development of its skill and intellect by becoming complacent and reliant on technology; and an unchecked entitlement, by both business and the law, to consumer personal information by virtue of providing a service, consumers literally, or figuratively through advertising, had paid for. In response, Apex slowly turned her focus away from her technology and investment businesses, and towards searching for furtive solutions to the growing conflict. Her decision put her relationship with Carter on a ledge, one they both desperately fought to keep from falling off.

"Marco Manuel knows a journalist has seen the files and a hacker has infiltrated Horizon, nice work," Carter said as he fell onto the couch and pulled Apex down with him.

"He knows and so does Secretary Davenport," Apex responded.

"Anyone else?"

"Not as far as I can tell."

"They're keeping the story to themselves. Interesting, but what next?"

"My guess is you are next. Have they contacted you?"

"No."

"Even more interesting. They have not yet told you your program has been hacked? What could they be waiting for?"

"Maybe they're trying to fix the problem internally."

"I don't like that idea."

"Neither do I. Means they are gaining confidence, independence. You should go home for a while. Keep a low profile."

"I don't think I have to leave."

"You don't have to be in D.C. to do what you're doing."

"I do if I want to silence Dallas Winter."

"Silence her? Really?"

"Well, I at least want to keep an eye on her for a little while longer. I do not like the fact she

might not have understood the warning I was trying to give her. Her writing has always been strategic national security stuff. I didn't think she'd want to get into a junior reporter's investigation of lost files. I might have to visit her in person to make her understand we do not need her help."

Carter sat up, his hands on Apex's arms as he pulled her body to face him. "No way. Confronting her in person is too risky. You have a face you know, someone might recognize you."

"I don't look anything like I did when we were first married."

"You do to me."

"Only because you see me every day. Hardly anyone else does. Don't worry," she responded, wiggling out of his hands and moving her body into the crux of his arm. "I know what I'm doing."

"None of us know what we're doing. At no other point in history have a group of private citizens, in public positions, worked to develop a system to monitor the entire world. We do not even know the legal implications of the entire process."

"The Attorney-General said 'go for it.'"

"Yes because the Attorney-General thinks 'it' is nothing but a discussion exercise. She has no idea the depth of permanent activity already taking place. One of my companies does the vetting for the software. On my flight here, I finally had time to read through their reports. And I must say, I am impressed with how much work has been successfully completed. I'm telling you baby, this thing is going to happen."

"Okay now you're freaking me out," Apex worriedly said as she sat up to face him. "How were a bunch of government bureaucrats able to move so fast?"

"Because GCS picked the right bureaucrats out of the whole lot of them. Marco and Julia are kind of diabolical masterminds. Together they plotted out a cover for every government department's contribution to the 2100 policy papers, which as we know is really the 21st century cyber surveillance rollout plan. Every department head assumed they were participating in a thought piece or policy research, and provided enough information and money to drive the project forward. With businesses, they essentially did the same thing. They gave CEOs and CTOs a few 'if' scenarios and asked for a response. With those two, each answer was also a roadmap into the company's potential complicity in the larger scheme. And on an international scale, Julia made the research a sort of competition for junior Foreign Service officers. She made these new kids in embassies all over the world think they each had a unique assignment from the Secretary to discover particular aspects of the host country's cyber infrastructure. Again, she worded the questions in a targeted fashion. Some of her officers even managed to obtain classified documents developed by the Chinese for local officials. The details explained how cyber security should be implemented for resource mines, ports, airports and even highway toll booths. Their results are extraordinary stuff. Another team put the information together in concise briefing documents. Those two have created a record unprecedented in history. Effectively their findings are the foundational blueprint for the connection of the entire operating world through the U.S. government, business and overseas missions. And you know, once the federal government is set, state and local governments will fall in line. The federal government can pay them, in the name of national security, to connect all of their servers to the national system. I'm completely stunned by their competence, the whole process is more developed at this point than we even imagined."

"You've seen all of these reports and documents?"

"Yes of course. Everything is on one of my servers. But as far as I can tell, Winter only saw the aggregated summary report and probability scenarios. I'm sure she's not aware of the sources for all of the information and the recommendations."

Apex stood up and moved towards the window, her face marked by tightened concentration. "Cart, we cannot let them build out this system. They've co-opted so many players and overwhelmed a bunch of complacent idiots who do not understand the implications of their plan. Putting the whole world under surveillance, can you imagine?"

"The project is more than the viewing coverage. People will be connected through everything they do. Any purchase made, banking, just using a cell phone will create a record of your activities in your personal profile in the central database. This is total infiltration of our daily world. 'The Internet of Things' now includes every human being...as a thing."

"*Cosa*."

"Exactly, Spanish for thing."

"But what will this 'thing' do to us as human beings? I mean will we become more trustworthy because all of our activities are recorded or more paranoid for exactly the same reason?"

"I think neither. I'm guessing most people will become indifferent to the world around them. You see their acquiescence happening already. Everyone likes to claim humans are social animals, but have you been on a metro train lately? Dead silence. Everyone has their ear buds plugging their ears and they are all looking down. In public, people barely acknowledge each other, they do not interact, every person is within their own...pod. In the future, when this project is completely rolled out and each human can allow the system to control personal movements, why would anyone make an effort when you can just wait for the system to spit out ideas and follow the instructions the program provides to you?"

Apex shuddered. "We can't let that happen. People have to be made to understand the system's true functionality."

"I don't know. People are pretty far-gone already. I'm not sure there is an opportunity to pull them back."

"There has to be."

"How?"

Apex considered a thought. "Maybe the media?"

"What do you mean?"

"Maybe I shouldn't be trying to scare Dallas Winter. Maybe I should be trying to build her cooperation."

Carter jumped up. "What are you saying? Don't even think about bringing someone else into our confidence."

"Relax and hear me out. Winter can help us navigate the media. Scaring GCS into believing they could get caught is another weapon against them."

"No!" Carter shouted in ramp anger. "Our weapon is technology. We use technology to defeat them in their tracks."

"Cart, from your own assessment, technology will not be enough. They can always buy technology. They can hire excellent programmers and build the tools they need to carry out their plan. If you decided not to help them, or they think your product is corrupted, they'll hand the software contracts to someone else. We have to scare them where it hurts."

"These people are not going to be scared. I just told you. They have set this implementation up to cover the country and the world, and they know the system has to be organized in a fashion

that can last long after they are gone. The entire foundational process has been laid. Soon Marco and Julia won't even be working on the details anymore. The whole project will develop on its own."

"How could a system develop on its own? You need drivers for this kind of roll-out, someone has to manage the process."

"Oh, they'll find someone to manage the administration, but the role will be secondary. The actual software, the ins and outs of the programming will be on auto pilot."

"What is this a Hollywood movie where the machine is in control?"

"No, the machine will behave exactly as coded. But the functions will include certain automated processes especially for transitions related to the expansion and adaptation to new technologies."

"Okay Carter, now you are freaking me out even more. You are telling me, a couple of government bureaucrats have been able to move COSA to the point where the system can manage itself, including understanding the impact of emergent technologies and how to implement advanced applications?"

"Not quite, COSA is not artificial intelligence. At this point in history, the system is actually human intelligence. I'm telling you, Julia and Marco are no one's idle government bureaucrats. They are two of the most extraordinary brains the federal government has ever had the fortune to employ. In fact, they are so good, they can do two major jobs at the same time. Julia can run State with her eyes closed, and work her team to move COSA along at lightening speed. What has happened here is they have established the foundation of the program to default into progressing with future technologies and operating with limited interference. The structure is like...like an NFL team, professional football."

"What?"

"The game adapts every time someone uses an innovative play or move on the field. You don't have to issue a directive, other players and coaches will copy successful outcomes. Sure the rules change, but only after the new moves and plays have been adopted. Julia and Marco have kind of built this idea into COSA. The system will react to repetitive behavior and success. The adaptations will come from measured outcomes. The response is not A.I., the system has been programmed to build upon its...actually our...own actions."

"Sounds like A.I."

"Not as I know you understand the term."

"But the machine will be executing on actions humans have not requested."

"Yes and no. The automation operates in a way we have requested, like receiving software updates on your phone."

"You can reject software updates."

"True, but I doubt you would."

"This is still a level of non-human decision-making over a lot of humans."

"I know."

"Humans who are not going to get the chance to vote on this outcome."

"Right."

"Even more reason to get Winter on a story to kill the system before the functionality really starts moving."

"Winter will be the one who will be killed."

"Oh c'mon Cart, you don't really believe GCS people are dangerous criminals."

"Unfortunately, I do. Suspend your beliefs about how people are supposed to behave. GCS

has been developing and planning a global program to continue without them. At this point in the implementation, any action taken to stop the rollout will simply be an exercise for the system's defenses. Any person who blows their cover will be eliminated. We cannot fight their plans in the physical world. Our only chance is through the technology. We must have superior technology, which comes through our brainpower. I've thought a lot about this and we have to focus on building the capability defense not for today's petty battles, but for the broader war to come. As the system gets built out, you'll be able to pick the pieces apart. You won't be able to bring the entire operation down, but there's nothing wrong with constant destabilization."

"You want me to let this thing...COSA...rollout without a fight?"

"You will be fighting. But attacking the whole structure will be useless. You'll have to settle for parts. Believe me, targeted attacks are the best we can do."

"I don't agree."

"I have more information on this than you do."

"I don't care."

"Why?"

"I think you've been spending too much time with your government buddies."

"Hey, wait a minute I hav—"

"You're feeding me the line they would want me to have. You want to see this system rolled out with your technology."

"That's not fair. I—"

"You're betraying our plans, Carter."

"No I'm not."

"You're betraying me."

"No!"

"You go ahead. See what you and your government friends can do but I'm not part of your surrender."

"C'mon A—"

"I think you should leave."

"You and I have a different li—"

"Leave right now."

Carter hesitated, but the look on Apex's face signaled a bitter anger in front of dense suffering. He could feel her calculating how much his words had taken away from the many other pronouncements he had uttered to galvanize them both towards a common goal. Considering his precarious position, he conceded to her immediate wishes. "All right I'll go, but I'll be in D.C. We need to talk. This discussion is not over."

Standing with her hands braced behind her on the windowsill, Apex did not reply. As Carter took a step towards her, she backed up against the wall. He stopped, turned and walked out of the room.

As he departed, Apex let out a deep breath and burst into tears. "Carter," she softly cried. "You have to understand, we cannot give up this fight." A minute later, wiping the tears from her face, she walked over to her desk, and picked up her mobile to call Dallas Winter.

*

"I know it's early out west," Julia apologetically stated to Carter over mobile. "But I was wondering if you are going to be in D.C. anytime soon, we'd like to talk to you."

Carter rolled over in his bed and glanced around the room. His eyes caught an unopened bottle of champagne and two dry glasses, and he suddenly remembered he had spent the night in

a luxury hotel suite in downtown D.C., without Apex, which had not been his intention. Sighing he said, "That's okay. I'm actually out east."

"Are you? How wonderful. By any chance, can you come to D.C.? The issue is one we could go over on a secure line, but if you're on this coast I would prefer to discuss in person."

"Sure," Carter replied as he stood and opened his curtain to view the gleaming white obelisk on the National Mall.

"When can you be here?"

Debating whether to confess his proximity or give himself more time, he took the middle road. "How about this afternoon?"

"Wonderful, we would like to send a car for you. Where will you be staying?"

"I'll have my assistant text the details."

"Thanks Carter, I'll see you this afternoon."

"Sure," he offered before disconnecting.

Gritting his teeth, Carter checked for overnight messages from Apex, but there were none. He sent her a morning greeting expressing his love and loyalty, before wandering into the bathroom to cleanup for his meeting with Julia.

The car arrived at the hotel on time and took Carter to Horizon to meet Julia in her office in the complex. Unlike Dallas, Carter did not need to be blindfolded, he had paid for the construction of Horizon and almost all of the equipment in the building had come from his company. Because he had wanted to experiment with advanced workplace technologies, employees in the building functioned with security measures that did not exist in any other facility. The innovations in biometric security scanning and the automatic elevator response details were his own code. When he swiped his key card, the turnstile indicated which numbered elevator would be available for the ride to his floor, how long before the doors opened, and based on all other requests up to that moment, how long the ride to his destination would last. The technology had been designed for super skyscrapers capable of propelling thousands of people in different directions around multiple building sites throughout the day. If he stopped to speak to a colleague, the chip in his card instantly updated the elevator information, which he could see by glancing at his mobile or tapping the card on a reader by the elevator door.

Arriving at Julia's office, he was immediately greeted by an assistant and ushered into the room.

Julia stood up from behind her desk and walked over to greet him. "Hello Carter," she said extending her hand. "Thanks for coming on such short notice."

Carter shook her hand. "No problem," he flatly responded. Julia motioned for him to sit down on the couch and she followed into the chair next to him.

"How have you been?"

"Great."

"Good. Are you out here for a particular reason?"

"I had someone to see."

"Are you staying long in the city?"

"I'm leaving right after this meeting."

"Oh well sorry, I'll drop the small talk and get on with the reason I asked to speak with you."

"Okay."

"Well Carter, the issue is a sensitive matter and I felt we should discuss the details in person."

"Go ahead."

"I'm afraid we had a breach here at Horizon. I was wondering if you could use your expertise to double-check our systems and confirm no permanent damage has been done."

"A breach?"

"Yes I'm afraid so."

"What kind of breach?"

"We don't know. We suspect one of our laptops was compromised and the damage may have spilled over into the whole system."

"Spilled over? Julia, this facility was set-up to avoid accidents. What happened?"

Julia briefly hesitated before confessing, "A reporter gave Marco Manuel a USB flash drive with documents appearing to be the 2100 policy papers. Apparently the drive was found in a restaurant. Marco put the device into his laptop, and the laptop went offline after displaying a message stating 'thank you.' He sent the laptop to IT to review and they cannot find any issues. We have not seen any problems directly in the servers either. But we are wary. I know you do not want to be called up for every little problem around here, but we felt this was a major issue and you had to be advised. If an incident arises you should be the first to know. Plus the equipment is all yours, if there is a technical error you are probably the one person who would be able to understand the impact."

Carter leaned back in his seat, and took a moment to ensure his voice displayed no identifiable emotion. "Well I appreciate your honesty. My team can check the servers and connections and let you know. But a reporter? What's this all about? What was on the drive?"

"The reporter's name is Dallas Winter, and she got the drive from a friend of hers who's a restaurateur, Fresno Tyler, the owner of Infrared."

"Infrared? Cool name."

"And a cool place. The restaurant is a very popular spot near the White House. Many elected and unelected officials frequent the establishment and many policy discussions can be heard there every night."

"And one of these restaurant guests had the 2100 files?"

"Perhaps."

"The real files?"

"Yes. Winter recognized the FedSec template used for the documents' format. And she brought her finding directly to Marco."

"Do you know who lost the drive?"

"No."

Carter narrowed his eyes. "Have you attempted to investigate where the documents came from?"

Julia shamefully twisted in her seat. In managing only Dallas and Tyler's access to the files, she had failed to focus on the number of other hands the information may have passed through. "No," she admitted.

"Wow. Negative publicity for this project is not much of a concern for you?"

Alarmed, Julia forcefully replied, "This project is my highest priority. You know better than to accuse me of downplaying an incident. We were focused on the people who did not know the origin of the files, Winter and the restaurant owner. We assumed the drive came from an insider who knew the content. The source could even be connected to our team. We would not have imagined multiple people would have had a look at the files before Winter handed the documents to Marco."

"But either way, you're not treating the breach very seriously."

"Do not accuse me of inattentiveness. Of course we are treating the incident seriously."

"Is there an investigation into the entire set of circumstances?"

"Yes, my investigation. You know I cannot conduct business around this project any other way. I cannot launch a large scale review of activities surrounding an issue only a handful of people know about."

Carter stood and walked to the window. "But you can launch an investigation? Aren't there controls on all file downloads?"

"Yes."

"You can tell which computer downloaded the files onto the drive in the first place?"

"Yes..." Julia hesitated, "...yes, I suppose."

"You did not know you have a function for reading file downloads?"

"Maybe not."

Carter turned to face her. "Julia, if we are going to be engaged in the most ground-breaking covert international digital infrastructure project in history, we're going to need a few rules."

"Yes of course. But the work we have already done was rapidly implemented. We really have not had time to focus on other details."

"Well you need to think about details now. You need to create an investigation protocol which should not involve calling me."

"I'm sorry Carter, but this was unprecedented and we have moved far ahead in the past year. Maybe we could consider hiring a permanent administrator for COSA."

"Permanent administrator?"

"Yes, someone to oversee the day-to-day."

"Managing the program cannot be an identified day job. The position would raise too many questions."

"We can create a camouflaged role, here at Horizon."

"For an outsider?"

"No, the job could go to one of us, but the work would be our only mission. One of us could resign our current position."

"We need you in your current position. Based on the information you hear or see around the world, we can make changes to the system immediately. A permanent administrator would add a non-influential layer we do not need."

Julia shrugged. "Well if you want more diligence..."

"You are supposed to be covering all of our bases."

"I realize that Carter, but I'm the Secretary of State for heaven's sake."

"You have 14,000 employees. Frankly, you really do not have to exert as much effort at State."

"That's unfair."

"Okay, maybe you have to be visible. But my point is, at State, you can arrange regular meetings and appearances as you see fit, and only deal with the major issues. COSA needs more of your time. Find a way to cover your actions however you like, but between you and Marco, we cannot leave issues dangling, like a reporter who mysteriously ended up with the 2100 policy files in her hands."

"Yes I know."

"What are you going to do?"

"About?"

"The reporter."

"The story is contained."

"But has she been neutralized."

"Not in the way I think you're assuming."

"Is she still walking around with a copy of the files?"

Julia stiffened. "I'm not sure."

Carter rolled his eyes. "I don't believe this. What are we doing here, Julia? Waiting to start an international public opinion crisis?"

"We have not had a chance to think about these issues. We've been too busy getting COSA up and running and ready to function on its own."

"Okay, awesome. But now we have to think about the consequences when someone finds out about the system before we are ready to reveal the story."

"To be perfectly honest Carter, as far as we are concerned, from now on a leak to the public is not ever going to be a problem for our implementation. The whole point of being singularly focused on the project's foundation was to make sure COSA could stand alone. Given the design of the underlying infrastructure, we are moving forward regardless of who finds out."

"Really?" Carter feigned a shock he did not feel and posed a question he did not need answered. "How?"

"The foundation we have laid, the detailed outline we provided for you in the last briefing papers, those features are under construction and almost finished. We have established every function to work autonomously. And given where we are on the implementation, I say if we have an issue with the press, we deny everything. If they decide to look into the details, their investigation will come too late."

"You mean at this point, COSA's infrastructure is so resilient, the system is going to be locked into place?"

"Yes."

"Even if the press has evidence of our detailed papers, and there's a public backlash?"

"The public can protest, but the system moves forward."

"You seem quite confident there will be no fallout."

"Look, anyone can create fake policy papers. The only reason Winter knew the work was ours was because she has national security expertise. She's a serious journalist, one who actually reads FedSec documents and attempts to interpret the meaning for her audience. But the average reporter would never have noticed the template nor understood its implications."

"If she goes public, the result will be her word against ours. But the documents have a high level of official detail."

"Yes, but we can still say the work came from another organization. Private parties write government policy ideas to reflect the government's implementation of new legislation. They are actually quite good at creating credible drafts, sometimes better than the bureaucrats. Look at the American Legislative Exchange Council. They write model bills for state governments to pass into law, verbatim. Astounding for a democracy, but elected legislators have abdicated responsibility for writing their own laws. A private organization does the work for them. We would have no trouble convincing the press a similar organization could have created detailed and readable documents for federal government action."

"Okay sold," Carter said with impatience. "If anyone asks, the documents on the mysterious flash drive are not FedSec documents. We assume an organization like ALEC drafted the policy in the hope of having legislators read the details and either debate or adopt the proposals."

"Sounds good."

"What else do we need to do to keep a lid on this story?"

"I'm comfortable we will not have an issue with Winter."

"I'll judge your confidence after my techs review the state of the servers."

"Fine."

"Anything else?"

"No. But Carter, I'm pleased you were in town. We needed to speak frankly and directly. Don't worry, I understand you may be concerned about our management of this unexpected distraction, but believe me, the program and all its secrets are safe."

"I'll take you at your word. We've come too far to have a slip up now."

"I agree, and we will not have a slip up later either. All of our plans will keep moving forward on schedule, as originally intended."

*

"Ms. Winter," a woman's voice reached Dallas over her mobile.

"You again?" Dallas disdainfully replied. "What do you want?"

"I've been trying to reach you live," Apex politely stated. "I would like to speak with you in person."

Dallas gripped her phone. "Who are you?"

"I'm a person with a battle to fight and I thought you, as a journalist, may be interested in knowing the details."

"What kind of battle?"

"One involving all of our rights and freedoms."

"Oh, sounds simple."

"It's not."

Dallas paused. "Okay where do you want to meet?"

"There's a coffee shop near your offices called the Conservatory."

"I know the place."

"Can you come there today at 2 pm?"

"Yes."

"Good, thank you."

"Wait. How will I know you?"

"I know you. See you this afternoon, Ms. Winter." The caller disconnected before Dallas could ask another question.

A few minutes before 2 pm, Dallas walked into the Conservatory ordered a macchiato and sat down at a table. A minute later a woman approached, placed a clear glass mug of green tea on the table and sat down across from her.

"Good afternoon, Ms. Winter," the woman said.

Instantly recognizing the voice from the phone calls, Dallas stared at an image matching none of her pre-conceived conceptions of the face behind the mysterious threats. The beautiful stranger was elegantly dressed in an expensive tailored suit. Briefly touching her immaculately combed back hair, she carefully placed a designer handbag on the chair next to her. "Good afternoon," she finally sputtered after soaking in the woman's exterior presentation from head-to-toe.

Ignoring the curious regard for her appearance, Apex asked, "May I call you Dallas?"

"Yes, sure."

"First I'm going to come clean and apologize for my earlier phone call. I did not mean to come off as the unrevealed antagonist of a suspenseful thriller."

"Oh I've forgotten about that already," Dallas lied, as she tried to reclaim her composure.

"You see this is a very fluid situation, and I did not want any incidents to occur that could move the needle one way or another."

"What situation?"

"The situation we are going to talk about. But first we need a common understanding. I am not speaking to you as a source for a journalist, you understand?"

"Yes."

"Do you have any recording devices turned on?"

"No," Dallas immediately answered.

"Were you planning to try and use one?"

"No, actually no."

"Okay, we're off to a good start. My interest in speaking to you is strictly to tap into your expertise about the media. The situation I'm going to tell you about is dangerous for the world, very dangerous. I would like to try and stop it, but I would need to understand how I could innovatively use media resources. I asked to meet with you to tap into your brainpower Dallas, not to enable you to write a story, you understand?"

"Okay."

"And you are okay with the ground rules?"

Dallas hesitated. "Depends on who you are and whether this situation you're referring to is real. If you're a credible person who is not wasting my time, yes I'm okay with the rules."

"I'm still going to tell you my name is Apex."

"Seriously?"

"I have good reason."

"Honestly you do not look like someone who operates under a spy name."

"Thanks I suppose. But I am a private person, extremely private and that is the crux of the developing situation we are facing."

"Okay what's the situation?"

"You remember the files you read on the flash drive you found at Infrared?"

"Yes of course. But how do you know I have that drive?"

"We have resources."

"Resources uncovering the late night discovery of a flash drive? That's a pretty specific task. Is someone looking for a missing drive or is it moving from hand to hand as you would have wanted?"

"I had nothing to do with how you obtained the drive."

"Okay, you didn't. But what about someone you know?"

"Not to my knowledge."

"You have no idea where those files originated?"

"Correct, I have no idea."

"Did you or someone you know follow Frez Tyler to my place the night the drive was found?"

Apex defiantly stared at Dallas. "Dallas, the content of those files, and more importantly, the broader story behind the creation of those documents is much more significant than the reason the drive was in the restaurant and ended up with you. I'm going to explain this to you and set a certain level of context, okay?"

Dallas narrowed her eyes, but gave up the fight for more details. "Okay."

"But you need to understand this information is beyond top secret. Think about a situation

where information is not top secret, at the highest levels of the government but...from them. The people who control the content on the drive are working outside government circles—"

"Okay Apex, hold up right there. Do you know how many people in Washington are telling fantastical tales of government conspiracies every day?"

"Hundreds."

"Yes hundreds. So whatever you are about to say—"

"Marco Manuel took you blind-folded to an office complex in the northwest quadrant, correct?"

Fighting an urge to shudder, Dallas answered, "Yes."

"You could see the Potomac River from the office you were in?"

"Yes."

"People used biometric ID scanners to enter and exit?"

"Do you work in that building?"

"No."

"What do you do for a living?"

"I own privately-held Internet companies through a silent investors fund."

"Where do you live?"

"Both coasts, depending on my work."

"Would I have heard of you?"

"I hope not. I'm serious when I say I'm intensely private. I think we should all have the option to protect ourselves from prying eyes. I find our current online world absolutely incredible. Our default personal information, the only unique identifiers we have are data we cannot replace, and its being tossed around as bits on the Internet as if the facts were worthless."

"You work in online privacy?"

"Not really, but let me ask you, when you were in Manuel's building did you notice the ID scanners?"

"Yes."

"Had you ever seen similar office ID anywhere else in D.C.?"

Dallas considered the question. "No...no, I don't think so."

"What else did you notice?"

"Just a lot of serious people walking in and out."

"In and out of which building?"

"The one I was in."

"And the other buildings?" Dallas thought back to her brief glance out the window of Marco's office, and suddenly recalled there were no people entering or exiting the other buildings. "Dallas, did you see any people at the other buildings?"

"No...no, I don't think so."

"No, you wouldn't have because the other buildings are a server farm."

"Sorry?"

"Buildings designed strictly for housing servers for data processing."

"Office buildings for data processing servers?"

"Yes, the concept is actually a good idea. The buildings are skeletons, there are no services, just reinforced floors for the servers. Building vertically allows for much more space and the maintenance costs are low. You only need to keep the place cool and dry. Options by the way that are severely lacking in a D.C. summer."

"Yeah, no kidding."

"But that's not the point. The people who bought the complex needed temporary space. In early 2008, businesses were scheduled to occupy the buildings, but the original tenants crashed along with the rest of the economy so the purchasers paid almost nothing for a shell. They configured the incomplete structure for housing servers."

"Who were the purchasers?"

"Private investors."

"What are the servers doing?"

"Churning through data. Your data and the private information of millions of others. They are developing the most intrusive technology tool we will ever know."

"What?"

"A complete surveillance and data integration program code-named COSA." Dallas looked skeptical. "I know I am sounding like the conspiracy theorist again, but you have to understand Dallas, some conspiracies are real."

"Okay, tell me about COSA?"

"Imagine total surveillance of everyone's actions, physical and digital, all the time. As I mentioned, a beyond secret process has been set-up to lay the foundation for implementing COSA across the country, and around the world. And I mean actually laying a physical foundation. They are going to build more server farms capable of using facial and body recognition to search through surveillance footage to find anyone on earth."

"Body recognition?"

"Yes, how you move, walk, stand, swing your arms. They are looking to be able to use those features to confirm identity."

"Why?"

"To catch bad guys, national security, take your pick."

"You mean if they have a suspect, this system would look at all surveillance everywhere in the world to try and find him?"

"Yes that's about right."

"But that sounds okay. I mean law enforcement is probably already using similar technology, this city has cameras everywhere."

"No, no one is doing this level of surveillance now. Cameras here and everywhere are recording the activity wandering by. But if law enforcement wants to see the video they have to know which cameras to search for and who to ask for permission to obtain the recording after an incident has occurred. In the future, the process will be reversed. They will have a suspect first, put the name in the system, and using face and body movement records, receive a data feed displaying the current and past locations of the suspect."

"But that sounds okay too. What am I missing? They will be working from information about suspects and evidence they have already identified to catch bad guys."

"Yes but searching for criminals is only part of the plan. To confirm identity, surveillance will be directly tied to all of your online activity, which in the future will be everything you do. I'm not talking about surfing social media and buying from an online retailer. In the future, you'll have your entire home and work life on an integrated system designed to track you throughout the day. Your workplace will be tied into the system, capturing when you are working and the tasks you are completing. Online activities can be cross-referenced to your physical presence in the world as identified by the cameras and sensors. There should be no more false arrests, at least not based on time and location, because the cross referencing of information should pinpoint the exact suspect."

"Okay I can see how the intrusion is increasing, but still I'm thinking the idea of catching criminals bef—"

"The system would know you, all about you," Apex angrily continued. "If you always do online ordering at one store, but physically like to shop at another, the system captures both data points. Everything you buy, read, see, everyone you talk to, where you go. The data would be aggregated to create a profile for every American, and eventually everyone on earth."

"A data profile for everyone on earth?"

"Yes, the initial set-up will work through the school system, or I should say online access to mandatory primary and secondary education coursework." Apex leveled her voice. "Besides the issues of failing schools, bullying, teacher bias, and rising costs, there is a basic threat to economic growth from the inability of the public education system to adapt to labor market demand. Thinking people realize the shortage of technologists will destroy America's ability to compete. One way to address all of those issues is to provide an interactive online education from pre-K to 12th grade. The idea would be to make the entire curriculum plus advanced placement courses available as a totally immersive interactive program of lectures, books, tests, exercises and a suggested study schedule. Children could begin at any time they are ready to start learning. There would be no set school year, no defined beginning or end time. Parents could schedule the learning day exactly against the hours of their own working and commuting time, and continue through the summer or other holidays based on the family's vacation plans. All the work a child does would be recorded. Instead of sitting in a classroom and being forced to learn at the pace of the weakest student in the room, each child would be operating at her own level. You could have a girl who is at an eighth grade math level, and a third grade reading level and that would be fine. Plus society would know, statistically at least, exactly how everyone is performing.

A lot of people will love the idea because more children could be tactically educated. Think of the desperate need for technologists, millions of unfilled jobs. But if the kind of kid who would be interested in a tech profession, the kid who can be on a computer all day, can succeed with an online education offering, those students can go through school quickly, qualify for higher learning and move into the working world. Silicon Valley may be the elite place to work, but America could use a dozen more high tech cities creating products tied to government or healthcare, policing and national security. We need ten times...if not 100 times more technologists than we have now. But there's no way we'll have the teachers available to make the push happen. And why should society wait for formally trained people to manage one classroom of 30 kids when we have the technology to move forward and have the same lecture series available to millions?

Education is a process used to provide a human with basic skills, such as reading and writing, required for operating in a modern civilization, and generating a common basis of information to be used as a foundation for future knowledge. Whether the objective is spread out over 2,000 leisurely days, or crammed into half that time, hardly makes any difference to the child's eventual standing as an adult who has retained the information. Think about a process without the organizational, social and logistical headaches of forcing every child through a common school system dealing with teacher foibles and rising administrative costs. Online education may end up improving focus, accelerating learning, instantly updating to changing labor demands, and saving billions in salaries and infrastructure through one sweep of a keyboard. Even if a fraction of kids could complete the online-only curriculum, the savings would be enormous, and the benefit to those kids would be incalculable. The idea has solid

appeal."

"But what about policing compliance? Kids would just cheat."

"You bring in controls. Instead of school buildings you would have study halls where paid monitors patrol the cubicles and maintain order. Of course every room would also have camera surveillance. A disruptive child could be removed and permanently ejected. For fraud detection, students could be required to report for testing at their current level, every 60 days or so, and if they fail to achieve a passing grade they would have to report to a traditional teaching environment for say, six months. The idea is to give parents and kids a level of learning flexibility no generation has ever had. The question will be: why are we relying on the whims of teachers when compliant computers could run the entire process for us?"

"What's the catch?"

"The catch is the battleground for a life online. Every child will end up surrendering their personal privacy and involuntarily creating reams of data for an online profile. A child's strengths and weaknesses would be automatically recorded and, one guesses, maybe an employer could have access to the information in the future. Also to make lessons more interactive, preferences would exist. For example if a student liked skiing, questions would relate to some form of skiing. But this preference would also be in the student's profile. The government and big business would know 'this kid likes skiing.' Suddenly your health care premiums go up, and you are bombarded with advertising for ski equipment and vacations in Aspen. The long-term danger of this whole idea is the inability to keep your personal data private. Your entire primary and secondary education performance, every second captured online would belong to the state indefinitely."

"A trade-off between privacy and efficiency, the core central battle of emergent technology aimed at consumers," Dallas noted, intrigued by Apex's assessment of the issue.

"Yes, but people have to understand the trade-off now. Because if past developments are any indication, in the future, consumers are not going to be asked to choose. The decision is going to be made for them."

"What do you mean?"

"The situation I've been referring to is already taking place. The foundation for building out the system has already started."

"But how? When?"

"Officially years ago, but functionally within the past eighteen months, they've kind of taken off with their plans."

"Who? How?"

"If you knew your government, or let's say private influential citizens, were engaged in a plan to co-opt your online data and create a national surveillance and activity database what would you do?"

"Reveal the story."

"And if they had plenty of options for suppressing the information, for claiming your story was false?"

"At least the story is out there, you raise awareness."

"Raise awareness?"

"Yes."

"Awareness and understanding are part of the challenge. The system will technically be voluntary but you have to opt-out, everyone will default in. Of course opting out will take effort, which most people refuse to exert. But those who stay awake and aware will make the

appropriate preference changes, and will not have as much information compromised as those who complacently give in."

Dallas leaned forward. "How much can you tell me about this whole project...to make this a story?"

"Dallas, what did I tell you from the beginning?"

"But your own alarmist words imply you want to make sure this system is publicized," Dallas protested.

"Not really publicized. I want to make sure the system is destroyed. Putting a story out there for the creators of COSA to deny will not destroy the system. Tell me what kind of pressure would have to happen to make them drop the whole idea?"

"Maybe a massive public backlash?"

"Against an officially non-existent project no one can see?"

"Okay, prosecution?"

"For writing policy papers?"

"I don't get it. I thought you said COSA was built."

"The rollout is too complicated to explain right now. But in general, the way the system was established makes the whole program appear to be a research and development project; benign thought pieces like the ones you saw; and a few experimental tests with cooperative government departments and businesses using old data. You can not point to a transparent project and say, 'okay we know where to aim our weapons.'"

"But if the project is out there and developed, how did that happen?"

"There are people who made the work happen."

"Okay what's the source of their power? In this town everyone hates to lose power."

"Would you believe their power comes from being incredibly smart, loyal and trustworthy?"

"You're joking."

"No, these are people who have basically outsmarted everyone, and in a really permanent fashion. Think about it. Most people, especially around this town, are idiots, operational idiots. They function in a narrow world of beliefs and understandings, plotting and planning their careers, seeking revenge against rivals and cheating on their spouses. The number of people who are true thinkers, who not only have a sense of duty but also actually aim to fulfill it, those people are few and far between in D.C."

"People like Marco Manuel."

"Absolutely. If you had a billion-dollar idea to drop into someone's care, you'd pick Manuel right?"

"In a second."

"Well, let's just say his skill is recognized worldwide."

"Wait. Really? But is he..."

"What?"

"Is he doing something illegal?"

"No, remember he is too smart to be obvious. The project is organized on a completely legal foundation. A private consortium is doing the prep work, and the government can eventually sign on, voluntarily without strings. All government participation so far has been conducted in the name of technological research. Almost every government department runs on two systems, or at least the employees think they have two systems, behind the scenes is actually only one."

Dallas shook her head. "Look Apex, why are you giving me a story I cannot use?

Especially if the project cannot be defeated. If you don't want to expose the truth, I don't know what else I can do. Writing the story will at least shake people up."

"How about you...you investigate the story."

"What do you mean?"

"Make your activities appear to look like you're going to write stories related to the documents you found."

"But won't that be dangerous?"

"Why? Was someone else threatening you besides me?"

"No," Dallas quickly answered, thinking of Marco's warnings. "But if they really care about their project they might become concerned about my sudden interest."

"You want that exact reaction to find a vulnerability. Let's see who decides to be concerned and why. Poke around a little bit on one topic, like education. There is already a lot of experimenting being done with computer learning in schools, pull a thread of the story, look at which computer hardware company is providing the most product to schools, who's got the contracts. While the basic curriculum is already available for home schooling, the next step will be the creation of advanced online tools, and whole communities demanding the transition away from their traditional, failing school. Try to see if the Department of Education or online learning businesses will reveal more. You write about cyber issues, an online education story should fit right in with your interests."

"I write about cyber security issues."

"Okay even better angle, 'are your kids safe?' People will freak out thinking about how criminals could get access to their children through online education tools. Exploit that option within the scope of your story. If the population refuses to complacently accept the concept, the system's backers will be forced to change the functions or they will not have a chance to succeed with their implementation."

"Okay, that may be a good idea. I'll think through a couple of possible scenarios but I'm sure one will stick."

"Okay good."

"But Apex, what exactly do you and I have here? A partnership of some kind?"

"I hope so, Dallas. I'll admit, I'm trying to get the system destroyed. You have to decide what's in this for you."

"You giving me the full story at some point. I'll wait for the details."

"I'm never promising the full story."

"I'll wait to see how much you will reveal. But can I ask now, why do you even know the details about this top secret plan?"

"I know insiders."

"Really?"

"Yes."

"You'll always have the latest information, like when the system will be fully rolled out?"

"Possibly."

"Will I get the story as soon as there is enough to reveal?"

Apex hesitated. "Revealing any part of the story may take years. But let's say, under any circumstances, you get the story before details are officially made public. And by public I mean a direct announcement about COSA or some form of the system's existence for public consumption."

"Okay, but in the meantime, can you give me another opening?"

"Like what?"

"I'm going to let you decide when the right moment appears. I can get people onto the questions about an online education, but you'll have to come up with another option before this breaks. I want to be the recognized lead on the details about the system and its implications."

"Okay, deal."

"And if there's trouble?"

"What kind of trouble?"

"The kind you were trying to use on me."

"Don't worry about any problems."

"Don't worry? Why?"

"I'll be vigilant, make sure everything is okay."

"How?"

"I think you already know. I have decent tech skills."

"You'll watch me? Trace my phone?"

"No Dallas, I'll watch them."

*

CHAPTER THREE - THE LAW ENFORCEMENT FILE

Carter sat on his own bed reading his Initium tech team's report about the security sweep at Horizon. The report was comprehensive in its condemnation. The building's sensors failed to note an unregistered flash drive on the premises; a file on the drive overrode the automatic security check on Marco's laptop; and the implanted program uploaded to the main operations system through the building's Wi-Fi connection. Every broken step in the process was a failing of his technology. Whoever had created the drive's files had utilized advanced infiltration applications he had never previously seen.

The approach Initium's confidential GCS partner team was taking to the assignment from FedSec involved a multi-tiered security protocol. The face of each person entering a Horizon building was scanned and cleared through a facial recognition application before a body passed through the entry barriers. Discrete sensors on walls and in doorways alerted for the presence of metal, wirelessly transmitting devices, miniature hard drives, cameras, recording devices, and certain drugs. All files originating on the internal system were digitally watermarked, and external files were flagged for viruses and suspicious code. Every desktop, laptop, tablet or mobile used within the premises had to be security cleared, which meant running a validation program to flag for unauthorized file uploads or downloads. And no one took work home. The office complex's servers contained applications for aggregating data pulled from government and businesses around the country. But the main COSA program was run from a server farm located in a converted decommissioned nuclear missile silo station near Carter's family home in North Dakota. As a test, more than 100,000 generated profiles had been created and the program ran analysis all day on updates of incoming data created by those 100,000 individuals as they pursued their lives. No citizen had volunteered for the experiment, but all of the data was legally obtained.

To protect their research advances in information collection, Initium's technologists were

convinced they could provide an unobtrusively secure environment where employees seamlessly walked around with their electronic equipment, and were unaware of the constant internal checks and verifications running against the devices they held in their hands. Horizon was the functioning test lab for their findings, but to Carter's surprise the bugs had yet to be completely ironed out. Annoyed by the report's conclusions, but prepared for questions, he sent the document over a secure line to Marco and Julia with only one data point expunged...the revelation about whose device was used to download the documents found on the flash drive discovered at the Infrared restaurant.

Feeling disappointed by his own shortcomings, he stood up, and in bare feet walked to the liquor cabinet to pour a glass of scotch. Moving towards the lights of San Francisco shining into his living room, he stood against a glass window and looked out into the city. 'Maybe Apex was right,' he thought. 'They could try to destroy COSA before the system completely rolled out.' But he quickly dismissed the idea. The minute the system was destroyed, a clone would emerge in its place. 'This advance is inevitable,' he thought. 'No government is going to give up on the idea of identifying every human within its borders.' And given that reality, thinking technologists should ensure the process was controlled even if they ended up complicit in the outcome.

Carter had no answer for the essential conflict inherent in his role. He was on the frontlines, playing both sides, manufacturing the equipment and coding the software to be used for COSA's infrastructure, and warning independent technologists to be prepared for the emergence of an advanced cyber enemy to fight. Neither stance felt entirely correct to him, yet he could not abandon either. 'How did the battle get this far?' he wondered. When discussions had begun between his company and the government, their intentions seemed only to be connected to national security. But the proposal had morphed into a vibrant project to permanently create a record of every individual. Not a criminal record, but a record nonetheless. The government's information gathering mandate was no longer the Social Security Administration having your birthdate and latest mailing address. COSA would know the presents you received for your birthday and if you were planning to move, along with the food you ate, clothes you wore, and each completed moment in transit from one place to another. The scope profoundly reached through the depths of an average person's life, and returned a kaleidoscope of information designed to aid government and business to identify operational objectives.

On the one hand, Carter welcomed the innovations. He considered the efficiencies and conveniences to be gained would transform people's lives and provide extended time for education, culture and recreational pursuits. But on the other hand, did government really have a right to maintain such detail on every citizen? Shouldn't the focus of technology be on security only, and those who may threaten domestic peace? Blanket coverage was designed to catch everyone, but at the expense of the majority innocent, law-abiding citizens.

Turning away from the window, Carter knew his musings were futile. Having provided money, equipment and technical expertise to build the program, he was already entirely implicated in the project's eventual implementation. His name would be hidden from history but he would always know the critical role he had played. In his lifetime the early stages of COSA would come to fruition, and he would clearly see the impact his handiwork will have on future generations, including his own children. 'All right,' he unenthusiastically conceded. 'I've made up my mind. I'm still with them. But where is Apex and what will happen if her actions are ever traced back to me?'

*

Two weeks later Dallas's first article, covering the impact of transforming public education online, appeared in the National Republic. In the article, she covertly speculated on the possibility of the initiative being encouraged by the federal government. Julia did not miss the insinuation, and immediately contacted Marco.

"So much for having Dallas Winter under control," she admonished him.

Marco had been stunned by the story and knew all too well the impact Dallas's words would have on his colleague and their plans. But he downplayed his concern to reluctantly reassure Julia of their position. "She is covering a legitimate story Julia, there is nothing to worry about," he responded.

"A legitimate story? She's trying to draw attention to our work."

"She can't draw attention to the specifics. She does not know what we're doing. She's speculating as journalists do all the time. There's an article a day about online education, no one will attribute unique significance to her words."

"But if people do, they will want to take immediate action."

"What do you mean?"

"You understand my meaning. People have worked long and hard to get to this point, Marco. No one wants to see even subtle leaks generated by your friends in the broader media. No one will accept being undermined by a reporter."

"And?"

"And action will be taken."

"Like what?"

"Like making sure she cannot spread the story."

"Julia, there is no story to spread. Dallas does not have our confidential information."

"You have to understand, Marco, this project has important sponsors."

"As I am well aware, but they will not notice suspicious words in a general story on online education. Only we know the whole story behind the story."

"The backers will not be disrupted in their plan to rollout on time."

"What have you done, Julia?"

"We have to make sure everyone connected to the process is protected."

"Did you tell other people about the information Dallas inadvertently obtained?"

"For the protection of COSA, our security is on par with national security, Marco. We have no choice but to defend our interests."

"She didn't do anything wrong!"

"Did you read Carter's report on the security breach at Horizon? You let down your guard with Winter and we have to face the consequences."

"She did not create the flash drive."

"Maybe not, but she has compromised our security by reading the contents of the documents. She is a danger to us, Marco. I'm sorry, but action has to be taken."

"What action?"

"Action appropriate to the circumstances."

"Julia, if you have authorized an action—"

"Don't bother to try and threaten me, Marco. You knew what could happen when this whole mess started."

While she was speaking, Marco turned to his laptop to activate a FedSec emergency protocol and sent agents in search of Dallas. "I can take action too, Julia."

"Don't try. You'll force questions to be asked where none should be forthcoming."

"I'll do what I can to protect an innocent woman."

"Protect yourself, Marco. Let me recommend, you protect yourself."

*

Entering her darkened apartment, Dallas moved forward into the hallway and nonchalantly reached back to switch on a light. A second later, a glove hand encircled her head from behind and clamped over her mouth.

Swallowing a scream, Dallas fought an instinct to hold still while squirming to face her assailant.

But he held her back tightly against his body and in his grip she nearly missed the strained sound of a man rapidly confessing, "It's me, it's me. Don't scream." Dallas twisted around in his arms as Marco let go and removed his hand. "Sorry, I did not mean to startle you," he hastily stated. "But I did not want you to scream or throw something at me."

Shaking in shock, Dallas backed up against her front door. "Oh my God!" she responded.

"Sorry, sorry." Marco took her hand and led her to the living room sofa. "Sit down." Dallas dropped onto the sofa and stared at Marco. "I'll get you some water." Marco ran to the kitchen and returned with a glass of water, which Dallas accepted with an unsteady hand.

"What are you doing here?" She finally managed to ask.

"Are you all right, feeling calmer?"

"I guess."

Marco sat down on the couch next to her. "I had to sneak in, sorry I startled you."

"What are you doing here?"

Marco took a deep breath. "What are you doing with the information you read in the fake policy files?"

Dallas stared at him. "You snuck into my apartment to confront me about the files?"

"What are you doing with the information?"

"Nothing."

"You wrote an article about online education."

"And?"

"And the speculative hints you added were mysteriously similar to the content of the education file in the documents you found."

"Is that a problem?"

Marco bristled. "You promised not to refer to the content."

"I did independent research."

"Don't split hairs, Dal. You are trying to draw out the writers of those documents."

"And if I was, why do you care? You said you're not the writer. FedSec is not the writer."

"I care because from the beginning you have associated the files with FedSec, and we do not want to be associated with somebody's random thought pieces about the future."

"And you had to break into my place to remind me of your concerns?"

"Yes. I cannot be meeting you all the time during business hours. And I cannot drop by and officially visit you at night. I had to covertly come over here to specifically remind you of your promise."

"I'm keeping my promise."

"Dal, your article is not a joke. You are trying to work around your promise by writing about the very issues you should be avoiding. Is gender bias in code up next?"

"No."

"Okay, one of the other topics? Either way, drop the idea right now."

"And if I don't?"

"Dal..."

"What's the real story here, Marco? You must have more because you would not go to all this trouble over a little online education piece if you weren't engaged in some kind of cover-up."

"Cover-up?"

"Yes."

"What are you talking about?"

Dallas hesitated. "I know there is a bigger story, Marco. I literally know and I'm not the only one. Why don't you come clean, be the one to break this wide open and we can have a proper public debate."

Marco narrowed his eyes. "I don't know what you are talking about."

"Marco, give up your plan and tell me the story. I can protect you, as a source."

"You're crazy, Dal." He stood up. "There is no story. And let me tell you, I am not going to accept your idea about doing an end-run around our deal. You publish another story containing content from those files, and I'll personally request the warrant for your arrest."

"For what?"

"You'll find out when you hear the charges."

"The files are authentic, right?" Dallas stood to face him. "The documents are not some policy speculation. The information is real, right?"

"No comment."

"You think your threats will stop me."

"Yes."

"Why?"

"Because FedSec has extraordinary resources, Dal. Don't make me use them."

"Go ahead Mr. Director, use the best you've got. Because I know about the project you are planning. I know about your unconstitutional infiltration into our personal privacy. And I'm not the only one. Go ahead and take me out if you want. But remember there will be others behind me."

Marco fought to keep his eyes from clouding over in shock, and his face from betraying his galloping concern. "You expect me to believe you shared this potentially explosive story with another reporter, no way."

"Go ahead with your theory."

"Be careful Dal, I will."

"I'm not afraid of you."

"It's not me you need to be afraid of. That's your challenge here, Dal. I'm not your enemy. Your enemy is not someone you can see. And you will realize too late, just how vulnerable you have been from the beginning."

*

Julia completed her eleventh straight appeasement phone call to a GCS colleague, sighed, stood and walked over to a cabinet where she had all the supplies to pour herself an adult drink. From the window inside her office at Horizon, she could see the flat tranquility of the Potomac River and appreciate the silence of this section of the city, which was a buzzing hub of waterfront activity during the day, and melted away into upper class passivity at night. Her mind reeled from the lectures she had been receiving from each caller. GCS's backers had established clear overall objectives for their alliance: keep democracy and free market capitalism moving forward; accept policies towards progress; reject failed ideas from eras past; promote individuals

striving towards their highest potential; guard wealth and prosperity for those who are willing to work for it; and fight back against anyone attempting to abandon, disrupt or end any objective of the mission. At its core, the mandate tactically covered maintaining an operational free market not with hope, but with industry, technology and a viable defense against those who were aiming to destroy their stability. In a world where human beings had the capacity to think, GCS members used their brains to a singular advantage. They determined that regardless of the vagaries of the democratic process, the pronouncements of media headlines or the chatter on social media, they would advance their own plans to ensure an economic and social atmosphere in which they could thrive.

Members met throughout the year in scattered small groups and private reunions aimed at solidifying freedom and wealth by uniting those who thought about independent action. Among themselves, people spoke freely about exactly how they would guard prosperity by, among other initiatives, building a cyber safety net across all of their government, business and social operations. The discussions initially began as distinctive aspirations, but emerged into determined pronouncements. The group placed no constraints of politics, culture, gender, ethnicity, seniority, media, or the law on its thinkers. And demanded in return attention, diligence, confidentiality and perseverance in exchange for a future employment contract designed to ensure their ability to continue to manage the project until the point when the secret died with them. Members understood the risk they were taking with their careers when they agreed to join GCS, and none thought twice about the importance of the broader external mission.

Returning to her desk, she called Marco.

"Hello Julia," Marco responded on answering.

"I have just spoken to about a dozen of our outside colleagues to reassure them about the project's status," she said.

"Why did they need reassurance?" Marco guardedly demanded.

"You know I have a duty to ensure our international cooperation remains in place."

"Fine." He paused. "Has everyone settled down?"

"Nominally there is fear, Marco. And when people are afraid, we have trouble."

"You made them afraid for no reason."

"No, I did not."

"What do you call your actions?"

"My actions were the needed response to an unsettling event."

"Really?"

"Yes, not all activity is related to you and your friends, Marco. In this case, I was responding to a story about someone telling someone else there was subversive discussion in hacker circles about the reach of our program."

"What?"

"And the hackers have much more information than Dallas Winter ever could have gathered from reading a few files."

"What information?"

"Basically the whole program."

"The documents from the breach at Horizon?"

"Perhaps."

"And it's legitimate...the details they've been saying?"

"Yes, the information has been disseminated much further than we could have predicted."

"But how and by whom?"

"We have no clear idea. But your friend Dallas has received a break. Our efforts now turn to the more definite problem on our hands, hackers, one or more with an agenda to expose our secret."

*

Apex lay across the couch in her College Park living room fielding text messages from independent technologist friends around the world.

'We should call ourselves the Cyber Defense League,' one of her colleagues wrote. 'We're going to be like a super hero group fighting for the rights of humankind.'

'No, Cyber Defense sounds like terrorists,' another protested. 'I don't want to sound like terrorists.'

'Maybe the People's Army,' another offered. 'Because we are fighting for the people.'

'I like a combination, Cyber Army,' another weighed in. 'We're defending cyber rights. We are fighting for cyber freedom.'

Apex looked up. For days, she had been advising her friends in the clandestine online world to be aware of the accelerating plans related to building a global surveillance and online tracking system. She did not give the COSA name for fear the word would leak out and alert FedSec that the idea was being circulated. But she encouraged her isolated colleagues to think of their profession as leaders in a defense force against planned government trampling of their privacy and civil liberties. Any cross-border negotiations or business plans aimed at globally unifying online tracking of individual activity were fair game for their list of suspicious government operations.

Separately, she organized the COSA documents to provide the background material her group would need to move forward. Unlike Julia and Marco, her friends would have to operate completely out of public view, preferably out of all views. But to stealthily manage together, they would need their own parallel online communication system, one not connected as a sub-layer within the current Internet, which people called the Dark Net, but as their own functioning independent infrastructure connected only when necessary to the public Information Superhighway. They would need to use narrow virtual paths allowing one-way access to the Internet, but no way back. Their portals would also have to be impenetrable to government searchers by virtue of invisible doors to which only they would hold the keys.

'To do this we'll need money,' Apex thought. 'But how can we raise money without being noticed.' Within a minute she thought of Carter but quickly dismissed the consideration. 'We are on opposite sides now,' she mused. 'He has succumbed to the demands of his government overseers and his help is unlikely to materialize in this fight.' Almost on cue her phone buzzed, and she looked down to see Carter's number reaching out to her as he had almost every waking hour since they had parted. Reluctantly, she answered.

"Yes," Apex guardedly said.

"Finally," Carter responded, exasperated, before quickly leveling his voice to gentleness. "How are you? Are you all right?"

"Yes I'm fine."

"Are you still in D.C.?"

"Yes."

"Are you coming home anytime soon?"

"No."

"C'mon..."

"Why would I come home? I have work to do. Many people are galvanizing against your illegal intrusion plan."

"It's not my plan. Are you telling people—"

"No. Not the details, only the general idea. I'm asking how we would prepare for the possibility."

"What are people saying?"

"Basically, we need our own internet, completely separate from the official one where we can communicate, trade ideas, even surf public Internet sites if we want. But in our world, no one's private data would be tracked for any reason. No one would be able to analyze your surfing history and determine which cereal to sell to you before breakfast."

"Sounds cool."

"Yes I agree."

"But?"

"Well you know...the usual issue, who's going to fund our intentions?"

"Who indeed?" Silence fell over them.

"Under normal circumstances, I would have asked you to contribute."

"What are normal circumstances?"

"You and I lying in bed and talking about our hopes, plans and dreams for the future."

"You can have that anytime you wish, just say the word."

"I can't have my desire while you are in bed with your government friends. That would be too crowded for my tastes."

"They are not my government friends."

"Who are they to you?"

"You know as well as I that I was asked to participate in a project of sweeping implication," Carter stated, his voice evenly strained. "When they pitched the idea to me, I saw an opportunity for my companies to weigh in on the basic security and infrastructure options that will govern our lives for decades to come."

"Sounds fabulous," Apex flippantly responded.

"You know as soon as I realized they were going to implement a global surveillance and tracking system, without succumbing to the rule of law or democratic vote, I told you the nightmare I saw coming and I encouraged your initial response to fight back."

"Yes you did."

"When I told you the other day this first phase was lost, I was being realistic. I'm not trying to sabotage you. I want you to realize the challenges you're up...we're up against. A couple of federal civil servants have aligned with global businesspeople and co-opted the extensive resources of the government, and in some cases, the world, to satisfy the requirements of their own plan. Marco, Julia, and the rest of them are running a private covert operation. I doubt this incredible depth of subversive behavior by government cabinet members has ever existed before. They have their own version of national and international security and they were able to move quickly. But you have flexibility and freedom and brainpower and you can move quickly too."

"What are you saying?"

"What would it take to build our own secret communication system?"

Apex was stunned. "You'll..."

"What would it take?"

"The physical infrastructure is straightforward, server farms and satellites. But everyone will want access to the public Internet without being seen. We'll have to create the software for

our required functionality."

"Do you know who could create the software?"

"Besides you?"

"Yes. I do not have time."

"Okay, yes I think I know who could do the coding or at least a few people who would try."

"Can you design a viable physical footprint?"

"Yes."

"Okay let's make a plan."

"Carter, I..."

"This should be a fair fight between people and their government. The process will likely take years but I want to do my part to level the playing field. And I'm guessing there are a few others like me who would be interested in the same opportunity to help."

"You're..."

"I know, I know, when am I going to see you?"

"I'm on my way home."

"Good."

"I love you."

"I love you too. Go design a secret internet for us and I'll see you soon."

*

"Hello Carter, sorry to bother you but I wanted to follow-up on a point from your security report," Marco said to Carter over a secure communication line recently re-developed for the offices at Horizon.

"Sure go ahead," Carter directly responded.

"Were you able to tell who owned the original flash drive and had access to the files before it was given to Dallas Winter?"

Carter did not change the inflection in his voice as he bluntly lied, "No, the investigation did not uncover a name. Why?"

"Julia's paranoid about some chatter from overseas."

"What kind of chatter?"

"Some hacker circles are talking about an idea sounding suspiciously like COSA."

"What hacker circles?"

"These are people State is tracking. Some are talking about a government idea that sounds like our idea."

"Is the chatter part of the same leak at Horizon, Marco?"

"To be honest, I don't know. But these hackers have a lot more information than Dallas had on the flash drive."

"Is their chatter about material stored at Horizon?"

"No, not completely. Hackers are hackers they could have picked up the information from anywhere. Any one of our sponsors could be vulnerable."

"This is unbelievable."

"Look, since you say we cannot trace the original source of the flash drive files, we can do no more except keep monitoring the situation and see where events go."

"Monitoring? What are these hackers planning?"

"We don't know."

"Any ideas?"

"No. What about you? Any ideas about what they could do?"

Carter was surprised by the question, but knew his myriad ideas were actual facts he could never reveal to Marco. "If they know about our plans their idea will be to sabotage COSA. They'll try and figure out how to hack us, that's what hackers do, and they'll go for the usual viruses and bugs."

"You think that's all they'll do."

"Sure, what other options could they have?"

"I don't know. I mean, I guess you're right. They're too independent and dispersed to actually organize a coordinated response against the physical infrastructure. But considering all the trouble they went to, I was thinking their actions might be more dramatic."

"How?"

"Well they've got brainpower but no organization. A bunch of guys in Russia, a few more in India, a couple in Silicon Valley - all of the talent to fight back but no common platform or approach. One advantage we will always have in this war is the inability of our enemies to function as a unit. We may get hit by one rogue technologist or another but I doubt the attacks would ever be in any prepared fashion."

"Yeah, you're probably right," Carter supportively responded. "How could independent technologists figure out how to get together?"

"They would need a communication system we could not find."

Carter laughed. "Imagine. Probably impossible to cooperatively and independently build their own operations."

"Of course it's impossible. Would cost them billions and they would have to hide the infrastructure from us. The functionality we're building is designed to avoid that very outcome...they are out of luck."

"Most likely. But are you prepared for the one-off guys you mentioned."

"Oh sure, those are the guys we are dealing with all the time. Of course we keep getting burned, but we're getting better. By the time our system rolls out, we'll be way ahead of them."

"You think so?"

"I know so. Rogue technologists are not going to catch us once COSA is up and running. Terrorists with bombs are not the only people we are looking for. We have to catch the online guys too. We will deploy COSA and absolutely neutralize their options against us. When we are set-up we'll be able to trace every digital signal and there will be nowhere to hide."

"That's the plan?"

"Yes certainly."

"Sounds good Marco, you guys are really ready."

"As ready as we'll need to be."

*

"I wish I could put a drone on her 24/7," Julia complained to Marco. "We need to know who she has been talking to." Dallas's second article about how a sharing economy website company for private room rentals was working on addressing the issue of racism in booking acceptances, had segued into an analysis about whether race and gender bias could be coded into online ordering websites. Several Internet companies had vehemently complained the suggestions in the article could not be attributed to any existing software. But civil rights groups equally protested the government needed to immediately formulate legislation to prevent the re-establishment of Jim Crow online.

Marco turned the front-page newspaper article over in one hand while scrolling through the social media traffic displayed on his smartphone, with the other. The story was quickly blowing

up in all corners with speculation as to whether Silicon Valley could implement a segregation agenda. He shook his head as he realized Dallas was challenging him to proceed on his threats. "I'm sure she was not intending this response," he said, downplaying his angry emotions.

"Yes she was. She's trying to create a story where none exists. She's trying to force us to tell her the details behind those policy files."

"I think she's writing about issues that are already out there. The space sharing company raised the racism issue as their problem. She did not create the idea. A couple of their executives were on some public discussion panel and brought up the difficulty based, I guess, on reported incidents."

"Were they prompted to bring up these incidents? Maybe by the threat of the story coming out another way?"

"I don't know. I mean, not that I know of."

"I wonder. She managed to exploit a completely separate issue to fit into her agenda about the document she had read. She's playing us, Marco."

"I don't agree. But what do you want to do about her actions?"

"If our law enforcement drone protocol was in place, I'd be following her with a camera right now."

"I think she would notice."

"Not in the future we're planning. In our scenarios, once unmanned aerial vehicles are used everywhere, my surveillance drone would be one of hundreds in the sky. The machines would be overhead all day delivering packages, assisting emergency rescue, handling manual labor, and gathering close up and detailed information for weather and the news. The rules will be straightforward. With our technology protocols, automated drones can be flown in any public space provided the machines are automatically tracked, noiseless, broadcast a unique signature, and are equipped with sensors to detect humans, birds, buildings, trees and other objects. And commercial drones can be any shape or size. Once civilians accept daily use, having drones as operational tools in law enforcement will be routine."

"The plan for law enforcement drones involves a lot more human rights issues."

"Yes I know."

"Police will be using drones as extensions of the human force, as 'flying officers.' Anywhere a human officer would normally, and legally, go, a drone could go too. But once the drone expects to engage with a suspect, rights groups will want the machine to come under manual human control. And the machines will be armed, weaponized. If the suspect is brandishing a weapon, the human operator can survey the entire area to ensure the safety of civilians before attempting disarmament. And the human officer can activate the drone’s weapons after assessing the situation as if the officer were there live. The impact on public order will be enormous. But you want to use this capability on a reporter today?"

"I would love to."

"I don't think the aim of our plans is to curb the first amendment."

"No, we want to track criminals...and suspects."

"What would following her with a drone get you?"

"A direct visual. A view over her immediate activities. Winter could be at the center of these rumors, she could be threatening our tranquil existence and we have no proof."

"Julia, with all due respect my friend, you're exaggerating her impact. Dallas is writing articles, not mobilizing forces against us."

"Those articles are a force. Unfortunately she's a good writer and people believe her

musings. Look at the civil rights groups jumping all over her latest piece. Had a single person complained about online discrimination through the website before she published her article?"

"Yes."

"Well they are crybabies. If you want to pay next to nothing to sleep in a stranger's house, you had better be prepared for the consequences. Welcome to the unregulated world. People can't have their cake and eat it too. You want a free market within the free market, you have to take your chances in exchange for a good deal. Home sharing is not subject to innkeeper laws for a reason, and everyone claims they want to operate that way, free of government interference. Well if they're honest, they should work out their problems free of government interference too."

"The home sharing industry is only one small part of the story. The bigger issue with online ordering is the potential for real hotels to pretend they have no vacancy; or clothing stores claiming no product because they do not want to ship to certain clientele; or delivery services pretending not to be capable of operating in certain neighborhoods. Instead of overtly refusing, the companies can use the software to display 'no vacancy' or 'out of stock' or 'no delivery vans available,' and instantly end the transaction."

"Fine, okay but we are not concerned with the emerging social issues, our problem is Winter fueling the flames."

"Dallas's story is not relevant. These issues were real before she published. Any noise you hear now belongs to the previous stories, not to her work."

"I'm not buying her guiltless defense in these reports. I want her interrogated."

"What?"

"FedSec can politely ask her as a citizen to come in for an interview. But I want to see her response to the questions you ask. Use our voice and body sensors to record her subconscious behavior. I want her on the record saying whether or not she is disseminating information about the files through her articles, and if she has had any contact with overseas sources who are revealing the information. If she lies now and we find the evidence later, we've got her."

"Julia c'mon, Dallas is not a threat to us."

"If she tells the truth and you are right. I'll take you both out to dinner. In the meantime, set up the interview."

"Julia, please."

"Marco, I hate to pull rank, but for GCS issues, you take orders from me. Set up the interview and let's see if your friend really is as innocent as you claim."

*

"Did he tell you the kinds of questions to expect?" an enraged Apex asked a troubled Dallas by phone.

"No, apparently I am being asked to voluntarily come in for an interview," Dallas replied, in panic. After one of Marco's assistants at FedSec had called to request she attend the interview, Dallas immediately called Apex for advice.

"Hmm, you should be aware they use voice and body sensor technology over there."

"Sensor technology? How?"

"They will look for changes in the inflection and pitch of your voice, and signs of strain or sweat from your body. You won't be hooked up to any machines, these are sensors operating invisibly in the room."

"You're joking."

"No, no I'm not. FedSec is about the only organization using the equipment. Of course they claim the procedures are experimental, but they use all the features."

"How do you know they use sensors?"

"You don't need to know my sources."

"Okay fine. But do your sources know what I can do to defeat this secret technology?"

"I do and it's not much. Without training on controlling your breathing and body temperature and involuntary movements, you will react as the questions are asked, and that's how they'll catch you."

"I have to be able to do something."

"Can you stop the interview? Why is this Marco guy determined to trap you?"

"I don't know."

"Did you piss him off?"

"No, we're friends."

"Some friend."

"If they catch me in a lie, can he lock me up? He told me the files were not FedSec. But can he now claim the files are FedSec's confidential documents, and I'm releasing the details in violation of some law I've never heard of?"

"Yeah like I said, some friend."

"But this is crazy. I have to get out of this interview."

"Talk to your friend. See if he wants to be flexible."

"Okay and can you try...try to see if you have any...any encouragement for him?"

"Me? How?"

"Don't people in your world...aren't you able to check..."

"What? Find some dirt on him online? A weakness we can exploit?"

"No!"

"Aren't you thinking of those possibilities?"

Dallas paused. "Okay, maybe a little."

Apex smirked. "Dallas, we are not the cyber mafia. I'm not going to put a horsehead in his bed."

"I wasn't asking for—"

"But since I'm personally curious, I'll snoop around a little bit and see if I can find useful information."

"Oh...okay thanks, I appreciate it. But really I was thinking about the technology. Can you do anything...you know, technically...to change the outcome."

"Oh, that's an interesting idea."

"Is it?"

"Yes, we like to experiment too."

"You do?"

"Yes we do."

"Can I—"

"No more words, my friend."

"Okay but is there anything I should do?"

"At this point, assume you have no option but to get out of the interview. Work on your friend. If he is really on your side, maybe he can prove his loyalty."

*

An hour later, Apex scrolled through a fact file she had created from trolling through the data gathered at Horizon. 'What makes you so suspicious Julia Davenport?' she thought as she read details on Julia's connections to GCS. 'You are the actual mastermind behind GCS and

COSA, and you have stunned us all with your efficiency.' Apex was impressed. She had not considered the Secretary of State to be among the elite who were formulating the implementation of COSA, until Carter told her about the advances she had made. Julia's position conveniently supported all the goals of the project's sponsors. At its core, COSA would be used to track down terrorists, especially across borders. Plus an entire globe under surveillance through a seamless system any global law enforcement agency could access would significantly aid every country's anti-terrorism fight.

Apex considered the implications of her findings. If the driving force behind the rapid implementation of COSA was Julia Davenport, then Apex's newly formed cyber defense team needed to stop her to slow the project down. Or even more lucrative, if they could get rid of her, cut off the head of the snake, the planned project rollout might be halted in its tracks. Apex weighed the possibilities. 'What would it take to remove the Secretary of State from her position and from GCS?'

Davenport's record was extraordinary. As a former Foreign Service officer, she had verifiable credibility among the rank and file, and as a former CEO who ran a successful business her leadership skills were rarely questioned. More striking, she had carved a global network of diplomats, policymakers, business leaders and financial investors who could open every door of influence. If Davenport suddenly disappeared, people would notice, and they would be concerned. The last thing Apex's group needed was attention drawn to physical activities in the real world challenging law enforcement's actions online.

Considering only the range of her previously analyzed options, Apex settled on calling Carter. Having returned to their San Francisco home, she was surprised to have rarely seen him since her arrival. Carter had disappeared into the challenges of his corporation. But Apex, after checking in with her top business lieutenants, retreated to her home office to pry through the Horizon files.

"Hey, I've only got a second," Carter said upon answering her call.

"I thought you wanted me home," Apex chastised him.

"I know, I know. The place has suddenly blown up. What do you need? I've really only got a second."

"I need to ask you about Julia Davenport. How possible would it be to replace her at State?"

"Completely impossible. She has the longest tentacles in Washington. She would basically know your plans before you even finalized the details. If you think that's an idea, forget it."

"My plans? Do you literally mean that?"

"Yeah, she has tech skills, don't underestimate her. She technically knows the type of security she has built on her home and office systems, and she was instrumental in moving the sensor technology to a broader rollout."

"Okay she's an untouchable superwoman."

"Pretty much. Why are you asking about her anyway?"

"I was just looking for a way to slow things down."

"I am telling you this project cannot be slowed down. Davenport made sure all steps are moving forward at rapid speed."

"I'm still looking at other options."

"Well stop looking and focus on the technology as we agreed!"

"Okay, okay, chill out."

"I gotta go, focus all right, focus."

"Yeah, yeah..." Apex quickly disconnected and returned to the files. 'Davenport has to have

a weakness,' she immediately thought, while ignoring Carter's warning. 'Our best chance is to uncover a shortcoming.' As she had done an hour earlier for facts about Marco Manuel, Apex sent out a '411' request for information text to independent technologists all over the world, asking if anyone had unpublished details about the life of Julia Davenport.

*

Shaking her head in disgust, Julia disconnected her call and contacted Marco. "You're not going to believe this," she said when he answered.

"What?" Marco asked.

"Someone is trying to find dirt on us."

"What! Who?"

"You want me to guess?"

"Don't say Dallas."

"Who else would be targeting us right now?"

"You're the Secretary of State and I'm the Director of FedSec. The list of potential people who could be targeting us is longer than the employee lists for our collective departments."

"Sure but that kind of targeting is a continuous stream of nonsense we vet every day. This latest search is much more sophisticated."

"Sophisticated? How?"

"Let's say I have a friend who does a little work behind the world scenes. This friend tells me a highly respected hacker has put out a call for information about us. There was no specific reason given for the request but this is the same hacker who apparently has been encouraging people to 'fight the power,' on the issue of online privacy."

"They are all talking about privacy."

"What did I just say? There's a connection to be made."

"A completely tenuous connection. What could they find?"

"I told you, I don't care. The issue is Winter and her agenda. You better be prepared for her interview. She says or does one thing to reveal her true intention to release those files and you have her arrested."

"Don't jump to conclusions. We'll wait and see how the interview goes."

"Be prepared, Marco. If there is any evidence, I want her gone. Do you understand?"

Marco sighed. "Yes all right, I understand."

*

An escort arrived to pick up Dallas for her interview at FedSec. This time she was taken to the organization's main office building near the National Mall. She walked in, eyes open to her surroundings and was directly taken to a room, windowless on three sides, with one-way glass on the fourth. The bare furniture consisted of a table, four chairs and a video camera. One of Marco's assistants greeted her and provided instructions before offering her a seat to wait. Several minutes later, another FedSec agent appeared. This one introduced himself as her interrogator, he would be asking the questions.

Dallas expressed no surprise that Marco was not directly interviewing her. With such formal proceedings, allegations of conflict of interest would be rife. Besides she assumed he stood on the other side of the glass, perhaps with a few other high-ranking officials who would be listening to her answers.

Sitting up straight and concentrating on a spot on her interviewer's face, Dallas listened to each question, waited a minute to compose her answer and stated a clear and direct response.

"Where did you receive the flash drive containing the documents?" the interrogator asked. After Dallas provided a brief but complete answer, he continued along the same lines:

"How did you receive the drive?"

"Under what circumstances did you receive the drive?"

"On the night in question, were you under the influence of alcohol? Drugs? Duress?"

"Had you previously seen the documents?"

"Had you previously seen similar documents?"

"Do you know what the documents mean?"

"Have you shown the documents to other people?"

"Do you plan to show the documents to other people?"

Three hours later, Dallas was permitted to leave. She did not see Marco or any other apparent senior official as she followed her escort back to the car and accepted the ride home.

At FedSec, Marco and Julia replayed the interview over an encrypted conference call with Carter. The voice and body sensors had detected no signs of stress, a reading Julia attributed to preparation, which Marco denied. As the repeated questions and answers continued to completion, the listeners held their comments.

"We played the interview for you to help you understand the breach we believe has occurred," Julia stated to Carter after the recording had finished. "The sole purpose is to allow you to express any concerns you may have and we will deal with them. We do not want you to feel at any time that we are not responsive."

"We also believe," Marco firmly stated. "This...breach, if we wish to give this incident a name, was not material. As you have heard, Winter has very little information."

"Yeah, she could be a really good liar, but in general, I guess I'm not alarmed," Carter responded, to Marco's relief. "Whatever she read is not directly connected to our work, and from her answers, pretty much sounded like she did not have any additional information."

"You really feel that way?" Julia asked incredulously. "She's running a campaign through her writing to reveal the contents of the documents."

"There's not enough in her answers to prove that accusation."

"There's more than enough to take action."

"If we take action we might draw attention to ourselves and risk scrutiny we do not need."

"We are already receiving scrutiny because of her."

"Not in a threatening way. Arresting a high-profile journalist for writing about documents we claim are not ours would be a much more direct risk."

"But we do not know the depth of the threat she has unleashed."

"And we don't need to create attention where none should exist."

"If I can intervene," Marco firmly stated to break up their bickering. "As of this very second, no people but us have noticed any connection between Dallas's reporting and our program. FedSec has not received a single request from any other press or organization asking for comments about her work. Nor have any internal departments or external businesses asked for more information. No suspicion has been ignited."

"FedSec is not mentioned in her articles, but other government departments are taking feedback," Julia clarified. "Officials are being asked to comment on the content of the articles, and to provide more information and insight into the possible connections to the government."

"Right, but since most government departments participated in the initial research and development they have answers for those questions. They know policy papers have been prepared, and they know people are speculating about future government initiatives and plans.

No one is surprised. We also have not heard about anyone going back to the restaurant, to Infrared, to claim the drive. Dallas asked the restaurant owner, and no customer has been looking for property lost on that night. Which means we cannot see an agenda with whoever had or saw the documents. I think we can agree, we are safe."

"We are not safe."

"Okay Julia, I disagree. But even if trouble were looming, the focus of our efforts should be our financing and build-out schedule. We have said many times we are setting this system up for the long-term."

"I agree, but a prospective view should not mean we are not vigilant."

"Of course we're vigilant," Carter insisted. "But we are also smart about how we use our time. Marco is right, let's switch to the financing and infrastructure build-out. We need our foundation to be stabilized or all the other discussions are useless."

Fuming Julia declared, "We have nothing to discuss on financing and infrastructure. I have both programs under control. But if you two find those topics more important than infiltration and sabotage from external forces, I'll leave you to discuss the fine points. I have other work to do, if you'll excuse me." She rose to depart.

"Julia..." Marco cried, holding up a hand to her as she prepared to leave the room.

"You both know how to reach me." She turned and left.

Carter let out a sigh. "Guess she's a little unhappy."

"She's very concerned about this project, and any potential fallout if our true intentions were ever revealed."

"We are all concerned about leaks, but she seems to have another issue. What am I missing?"

"Nothing."

"Julia is extremely smart and knows this project better than anyone. If she has insight we've overlooked, I want to know."

"There's nothing I'm aware of."

"All right, but still, talk to her, find out if there's more to her concerns. I do not want any surprises. And I don't want her pissed off."

"Yeah sure, I don't want any surprises either. We've come this far with our objectives, the next steps are critical to making sure we finish and win."

*

No further articles emerged under Dallas's by-line as Julia decided to respond to her own instincts by doubling down on her efforts on behalf of the project and accelerating the implementation timetable. "We have sufficient detail to present the blueprint as is, to the current group of world political, business and law enforcement leaders," Julia said to Marco. "We are ready to move. This year, not next, we take the outline of the experiment to the President."

Marco bristled. He had never wanted to involve the President of the United States in the project plan. With only four to eight year governance mandates, a democratically elected American leader did not have the control or influence required to ensure COSA was accepted and implemented over the long-term. "Aren't we being hasty?" Marco cautioned. "We do not need to take any details to the President so soon."

"I've had enough of waiting to be exposed by forces we cannot control. Once the President completes his portion of the work, we will truly be on our way."

"What exactly are we going to tell him?"

"We say we have a functioning deal involving multiple enthusiastic participants. We are

informing him of the existence of COSA, as an experiment in global surveillance. The U.S. government is not quite paying for the system. No legislation was required to pursue research in the field. We have only utilized existing resources to merge online databases from businesses and government to test for efficiencies."

"I'm sure the legalese is paper thin."

"You only need to worry about the law if there is someone planning to challenge your actions. COSA fits neatly into all of our administrative mandates. And the system can be reconfigured at any time to comply with government directives. The current existence of the project transcends time, all we needed to do was make sure there was a base to stand on and we have built one. The information the President will receive is simply an advisory. There's no wrongdoing if private interests create a service the government later decides to use. We are going to present the details to the President in a format highlighting the voluntary and experimental connection to government departments. He can take the data to the G8 and NATO meetings, and ensure other world leaders understand how their voluntary participation would be appreciated. Once everyone has signed on for the experiment, we can cement COSA into place and the system will be set forever."

Although the President was expected to attend both the Group of 8 and North Atlantic Treaty Organization summits in Europe later in the year, no separate cyber security briefing had been prepared to include COSA and its experimental mandate. Instead, Julia was expecting his advisors to accept her recommendation to have the President informally announce the program to the allies, and seek global support.

"Does the President understand the implications?"

"His staff has to brief him. We provided all the materials, we do not need to take further action."

"Are we expecting G8 and NATO cooperation?"

"Yes of course, the groundwork has been completed."

"And you're okay with all of the plans, and the current state of our...our situation."

"If you mean your friend Dallas, some unknown hacker and the other forces challenging this project, no I'm not okay with the situation. But I've been too busy making sure we are ready to worry about their feeble attempts at sabotaging us."

"Okay, okay...we are set. A global rollout is a *fait accompli*."

"Yes, we are set. We are finally ready for the next level."

*

Although the breach at Horizon had provided Apex with a trove of valuable information about COSA, she was still searching for the program's detailed development plans, especially the outreach to global leaders, businesses and other organizations capable of participating in the project. The faster GCS was able to claim more adherents to COSA, the harder the system would become to dissolve. Each entity could act as another's redundancy, making a data breach at one facility only a temporary operational blip on a company's time. Apex needed to ensure she exhausted all options to inflict permanent damage or at least debilitate an organization's COSA connections. With security at the Horizon offices re-established by Carter's cleanup, she had to consider an alternative route to GCS's confidential data, and decided one may exist through the electronic devices Julia and Marco juggled between home and office.

In the build-out of electronic gadgetry into consumer uses, people had already sacrificed security for convenience. Even high-ranking government officials responsible for cyber security were vulnerable to the appeal of innovative personal devices rapidly adapting into popular use, at

the expense of outmoded models favored by internal electronics experts championing a rigorous security blanket. Given the variety of options used to access confidential documents, Apex hoped to find a breach by cross-referencing Julia's personal mobile, tablet, home laptop and main office desktop at the State Department with the same devices owned by Marco, and identifying an opening a clever tech could enter. Government departments were notoriously weak with their technology protection infrastructure. With millions of technology jobs left unfilled by the lack of attention to science education specialties, all sectors competed for the few graduates and experienced programmers who were available to work. But a hierarchy of preference had developed in the talent search world. Qualified and coveted technologists usually preferred first to accept positions offered by innovative, driven entrepreneurs either founding their own companies or going to work for those who were coming up; next option were the established Silicon Valley technology companies and competitors in other cities who could provide sufficient benefits and steady pay along with free lunch and recreation; those searching for high salaries in exchange for time-consuming work weeks turned to management consulting and financial engineering; then the government appealed to the patriotically-driven or selected from military-mandated assignments; until finally at the end of the line all other industries, non-profits, education and other government departments waited for the few available hands who would be willing to launch their careers in organizations where neither high pay nor prestige would be readily forthcoming.

Within the cut of desperation among the government departments, Apex expected to find a mistake. She only needed one deficient path, and she could be in on their systems within minutes. Running a series of proprietary search applications developed by her own companies, Apex leaned back to take another look at the documents Dallas had uncovered, and contemplated the uphill battle lying ahead.

With some plans, the government would always be able to claim the conveniences and efficiencies of COSA far outweighed any potential concern about privacy. In the consumer file found among the policy documents on the flash drive, GCS was proposing unlimited access to financing for consumers who defaulted all of their personal banking and investment information to COSA. The functionality's appeal to consumers would be overwhelming. In the distant past, traders had to rely on physical property as a medium of exchange. Pure gold had been the standard used by all nations as absolute proof of financial viability. When governments determined they could print money without restraint, paper became the mechanism through which they built developed economies using only the whimsical acceptance of high finance currency arbitrageurs as the definers of fiscal value. For the future, physical currency would disappear from the public's view, and the paper dollar would be replaced with digital accounts displaying the availability of funds to pay for services using vaporous digital code as the intermediary. Under COSA, the system would extend credit far beyond the balance available in an account, without spending limits. If an individual's checking or savings balances fell to zero, the system would automatically search the entire Internet for available sources of loan funds. Based on the consumer's personal data including education, employment and prior loan histories, a program would scan thousands of offers from all forms of lenders, all over the world, and extend a line of credit or a short-term loan. The consumer's pre-defined prerequisites, from a cap on the amount borrowed or annual interest rate, to the location of the funding institution, would define the parameters for an acceptable lender. Once the account received approval, before the next bill was due, the system, without input from the consumer, would transfer the funds, and spending could continue with impunity.

'This will be the ultimate crutch,' Apex thought. 'On this governments would grab every last consumer. Who wouldn't want access to an endless stream of funds?' The proposal did include the need for qualifying criteria and interest rate controls. But for a consumer who previously had no access to credit, the system would provide an automatic, no document, no approval, no wait lifeline, even at a 400% annual interest rate. Apex shuddered. Borderline financially safe consumers would succumb to the offers in the name of security and desire at the same time. Apex imagined the excitement around the release of the application, rolled up with these features designed to simplify a life and remove all known sources of financial stress with the click of an 'I Agree' button.

'These plans are a diabolic mix of efficiency and the invasion of privacy at the same time. Online education, sexist code rules, drones...' Suddenly Apex recognized an option she had not yet contemplated in her attempt to infiltrate FedSec. 'Drones.'

Turning to her laptop, she began searching for the home addresses of Julia and Marco. Julia's address was not in the files Apex had co-opted from Horizon, but remarkably Marco's was, and with his coordinates, Apex realized she had another opportunity. Maybe she could enter Marco's home with a drone, use the machine to locate his cell phone and directly access FedSec through his personal device. Looking next at available drone sales options, she selected a model available through an online-only outlet, paid for overnight delivery and waited for the machine to arrive.

Commercial drones were generally considered toys for hobbyists extending the reach of model airplanes by adding a camera to provide a literal bird's eye view to humans on the ground. But the media and the public widely speculated on the myriad potential additional uses for the devices in tasks from search and rescue to childcare. The only limitation was government regulation, which, as always, lagged behind the actual real-time uses people were already practicing. The drone Apex ordered was shaped like a mini-helicopter with a flying saucer belly, and equipped with a camera for remote viewing, and two claws for grasping objects. After assembling the loose parts, Apex tested the machine in her small living room. Placing her mobile on a table, she stood across the room and looking only through the camera's video feed, flew the drone to hover over the surface, and attempted the manual manipulation to pick up the device using the grasping claws. A second later, she lost control and dropped her phone to the floor. "Damn," she remarked aloud as she set-up to try again.

As night turned into early morning, Apex ran the maneuver over and over again. Placing the cell phone at different angles and on varied surfaces, she made certain the claws could quickly grasp the object and hang on for an extended time. As the sun began to rise, she concluded her skill was sufficiently perfected. The grasping claws were an unfamiliar, added feature requiring additional practice to raise the probability of success. But as she crawled into bed, another thought drifted wearily into her mind. 'I hope Director Manuel sleeps with the window open,' she told herself before succumbing to slumber.

Departing for D.C. after 1 am, Apex drove the lightly-trafficked streets into the city and left her car parked in a vacant lot three blocks from Marco's building on the edge of Mount Vernon Square. Scouting the location, she noted the nearby rooftops and calculated the ease of access based on residential traffic and security controls. For her task, she would require limited observers and compliant overnight guards, but D.C. was blanketed in surveillance cameras and vigilant eyes. Carefully scouting for two available rooftops near his building, one to hide the drone, and the other to hide herself, she selected views, which on sight did not appear to cross any lines capable of triggering an alert before she could complete her task. Separately, she

hoped Marco preferred to doze with fresh air, but as she trained binoculars on his condo's exterior, she realized the windows were closed. Scanning over to his balcony, she zoomed in and discovered he, probably without realizing, appeared to have left the door open. 'That will do,' she contentedly thought. Satisfied with her physical surveillance, she returned to College Park to await the ideal night for executing her plan.

Around 2 am on the night of her attempt, Apex arrived on foot to the quiet street running along one side of Marco's building. The early morning hour was not quite late enough to be devoid of all human presence. But walking within a cover of trees, Apex decided the few people milling around were unlikely to notice her. Most were drunken college students or drug-affected homeless wanderers. With the neighborhood's close proximity to well-touristed zones, a few late night strollers would not represent a threat to her personal security. Intending to avoid being seen launching the drone, she made her way to the rooftop garden of the building where she would hide, and activated the drone, which had been carefully hidden a day earlier on another building's under-utilized rooftop. For both entries, gaining access to the roofs had only taken a few minutes of eyelash-batting pleas. D.C.'s obliging building security guards conveniently had only helpful aid to provide to a purported tenant who claimed to have lost her key.

Using binoculars to peek through Marco's blinds, Apex determined he was asleep. Comfortable she had her opening, she accessed the drone's remote control and manipulated the machine off the roof and towards Marco's balcony. Too late, she realized the balcony door was closed. She had not practiced opening a door with the claw and worried about the add-on feature's pulling strength. But with a closer inspection, she noted the door was only aligned with the doorframe and not secured at the latch bolt. Locking the claw on the handle, she required only a slight tug to pull the weight all the way open. Smiling with relief, Apex flew the drone into Marco's apartment. Looking at the camera feed, she scanned the common areas, maneuvered into his short hallway, and seeing another open door, flew into his bedroom. The drone was not one hundred percent silent, and Apex had no idea if Marco was a heavy or light sleeper. But she would not wait around to find out. Inside the bedroom, with street lights from outside beaming strips of brightness across his walls, she immediately scanned his side table for the phone, which was openly displayed where he could reach for it, but also, to her alarm, plugged in.

"Crap," she cursed. The claws would have to hold their own against a cord plugged in to a wall socket. The feature had the clasps for grasping but may not be able to defeat the resistance created by a connected cord. Moving the drone over to the table, she easily used the claws to pick-up the phone as she had practiced, and started to fly away, cringing for the moment the cord would yank back on her pull, which was only a minute later. Thrusting up her drone speed, and the noise, she moved the machine back and forth with abrupt jerks trying to wrench the plug from the socket or alternatively from the phone. After three attempts, she opted for maximum speed and with one last tug the cord released from the wall, but the plug abruptly dropped onto the side table with a clang as the metal end hit a glass of water.

Marco stirred and sat straight up in bed. Quickly adjusting his eyes to the darkness, he caught sight of the drone flying out of his bedroom, clasping the phone in its claw, and dragging the dangling electric cord like a tail waving good-bye. He leapt out of bed.

"What the..." Marco yelled, chasing after the drone. As the machine raced to the balcony, Marco tried to reach forward and grasp the cord, but the drone slipped through the open door and took off straight up into the air while securely holding the phone in its grasp.

Apex had planned to land the drone in the empty parking lot where she had parked the car

five blocks away, and she ran to the location while listening for the sounds of sirens building towards Marco's building. Arriving at the lot, she maneuvered the drone down, grab Marco's phone, and threw the drone and phone cord into the car trunk. Flipping open her laptop, she hurried to use the phone to enter FedSec's computer system before Marco could reset all the security codes and trace the phone's location. With perhaps seconds to spare, she was in at FedSec and downloading the detailed preliminary plan for COSA and the President's briefing papers for the G8 Summit. Triumphantly, Apex shut down her computer. Opening the car door, she dropped the phone on the ground and smashed the device five times with a sledgehammer. Satisfied, she raced out of the parking lot and drove back to College Park with her captured personal copy of the elusive details for the most comprehensive electronic surveillance plan ever developed.

*

CHAPTER FOUR - THE CONSUMER FILE

Marco paced his living room floor while a team of investigators recorded the scene for evidence. Watching their activities, he knew the work was fruitless. The theft of his mobile phone had been brilliantly executed. No clues to the perpetrator would be found at the physical crime scene, the more viable search would be online, as the technologists looked for breaches in FedSec data to find the information the thief had stolen. Marco actually had three mobile phones. He hung on to one for the number he used from his last employment, and another global number he used for personal travel, but neither device was equipped with the security measures downloaded to his primary FedSec phone. And his main device, the one he kept by his bedside, contained all of his contacts and access to FedSec and other confidential government sites. Although he knew the phone carried proprietary FedSec security protections, a talented hacker could override its capabilities in a matter of minutes. The system had been tested with cooperative independent technologists who had shown his security people how external access could be attempted, but the preventative upgrades they had developed had not yet been implemented.

As an investigator approached to provide him with a summary of the situation he had already guessed, Marco stopped pacing to patiently absorb the details. The team had failed to determine the location from where the perpetrator would have operated the theft. And the type of drone model was also unknown. But based on Marco's description, they could narrow down the options and look at recent sales. The addition of the grasping claw was intriguing but not conclusive. They explained the functionality was an emerging feature and could help identify specific models equipped to attach the accessory. But to remotely manipulate the claw, the drone's camera had to revolve with the ability to look downwards and sideways. The perpetrator would be someone skilled with the equipment. Marco nodded and dismissed the investigator, the information would not advance the case or provide him with the insight he needed.

After providing another investigator instructions for closing up his apartment when they finished, he retreated to his car and drove to FedSec. Entering his office, he logged into the system, requisitioned a replacement mobile phone, and called Julia from his secure landline. After telling her details of the theft, he waited for yet another condemnation of his lack of care.

"Think about the implications of thefts by drone," Julia sympathetically responded. "No fingerprints, no digital trail, no sighting of the perpetrator, it will be cleanest crime a criminal can pull off...until COSA is built out and every drone is on the system or picked up by sensors."

"Well our covered future does not help me now," Marco angrily responded. "The claw on the drone opened my unlocked door. I'm on the 15th floor, I could never have imagined the scenario of a drone coming in through my balcony."

"No, of course not."

"The preliminary security analysis says my mobile was used to access FedSec files. The perp went after the COSA blueprint."

"We should have guessed."

"The whole document is in another set of hands."

Julia paused. "Well as annoying as that revelation is, a theft is not the worst outcome."

Stunned, Marco asked, "Why? How are you not concerned?"

"Oh I'm concerned, but we've moved on, Marco. COSA is in implementation and no longer in discussion phases. Whatever the perp thinks he's going to do with the blueprint will come too late."

"But he'll have incredible insight."

"That's okay, he won't have the program code. If your thief was a hacker, he cannot get in to the actual system with the information contained in that file."

"But he can publicize the blueprint. This time he can say he has a legitimate FedSec file and pretty clear evidence. I called the city police, the theft is public record."

"We can still deny the intention. We can repeat the entire idea is a research project with no official mandate, which is true. The blueprint does not indicate where and when COSA is to be implemented, nor do the details state which department is responsible for laying the foundation. We are on our way with this project, Marco. Whoever stole your phone waited too long to execute on a well thought out, but poorly timed crime."

"You don't think the theft is a problem?"

"The perp has literally picked up the roadmap after the asphalt has been poured. We're okay Marco, don't worry. Go home, sleep. The project is done."

*

"Someone stole Marco's cell phone," Dallas said to Apex over a call.

"You have to be careful in Washington, the city is not really safe," Apex nonchalantly responded.

"Where were you last night?"

"Me? You think I am a thief?"

"Well no, but maybe one of your people?"

"I don't have people."

"Okay, what do you think the thief will do with Marco's phone?"

Apex laughed. "What can't one do? Smartphones are great leverage into a person's life, especially the head of FedSec. One innocuous e-mail address could be the key to opening a dozen doors. Manuel should have been more careful."

"I don't think he was expecting a drone to fly into his bedroom to steal stuff."

"A drone? Well, people should assume that development was inevitable. No one really believes drones will only be used to deliver Amazon packages, do they? They have to expect criminals to come up with other ideas."

"The average person has not thought beyond the packages. Only people like you think about

broader implications."

"People like me?"

"Yes, I've...I've extended the reach of my investigation."

"Oh yeah."

"Yes."

"What for?"

"I was curious. There are not too many women who own Internet companies or investment funds, private or otherwise."

"Yes women are under-represented in those fields."

"But I was thinking about where I might have heard about women with those interests."

"And?"

"And I...I ran your face through the facial recognition software in my brain and searched around for where I thought I might have seen you before."

"Happy someone is still using a brain."

"Yes, well I recalled where I've seen you."

"Really?"

"Yes. When Carter Harden was first coming up as an Internet mogul, he was often photographed with his wife."

"Is that right?"

"Alexandra Spencer."

"And?"

"And I think that's you."

Apex burst out laughing. "Oh Dallas, you're funny."

"Are you denying you're Alexandra Spencer?"

"I told you my name is Apex."

"But you're her too?"

Apex laughed again. "What am I, a superhero with dual identities? If that were true at least give me a cooler name."

"Your husband has a few billion dollars. Enough to finance your...rogue hacker adventures."

"Well, well, listen to this traitor to the cause. I told you I'm a businesswoman with my own company and you accuse me of being a kept woman. Such a horribly sexist line of assumption to pursue."

"I apologize," Dallas shamefully said, instantly backtracking on her comment. "You're absolutely right. I don't know your net worth. You could be financing this adventure on your own. I honestly apologize."

"Do you?"

"Yes I do."

"Why are you even questioning me?"

"I had a memory. I cross-referenced my memory to online photos of Alexandra Spencer, and I came up with you."

"That's hardly valid evidence."

"I thought I would at least try."

"Why?"

"What do you mean?"

"What were you hoping to achieve by asking if I was Alexandra Spencer?"

"Just background."

"Or a story?"

"No."

"We've had an agreement since the beginning, Dallas. There is no story here."

"Yes, I know but—"

"No story about anything. About me, about the documents you found, about this so-called adventure you think I'm on, no story."

"Yes, I understand."

"I hope so because you should not be turning friends into enemies."

"No I shouldn't," Dallas contritely agreed. "I really do apologize."

"Apology accepted. And for the record, of course I'm independent and completely self-financing. I told you I'm a private person, and I want my privacy respected which, by the way, is not an outrageous demand. It's a fundamental American right, a constitutional amendment for heaven's sake. Do you know what year the fourth amendment was passed?"

"Ahhh...no."

"1791. Can you imagine? At that point in our early history people said, 'hey I have a constitutional right to be protected from snooping in my home, on my person, or through my papers and effects.' The right to privacy has been required by law for over two hundred years."

"But the Constitution only refers to government intrusions, not private."

"Yes but now the two are becoming one and the same. If the government is allowed to force private companies to give up their data, the action is a government intrusion."

"But reasonable searches are allowed."

"And who's defining reasonable?"

"Public opinion?"

"Yeah until the feds come looking for you."

"What made you such a major privacy crusader?"

Apex hesitated. "I believe in my individual rights. The idea of government viewing us as pawns to be played and manipulated has never sat right with me. I am a sovereign being. Government's sole responsibility is to keep crazy people away from me so I can thrive. There is no government role to manage what I personally do every day."

"But the government would say, safety comes at a price. You have to allow them to protect you by implementing universal procedures covering everyone."

"Violations of privacy in the name of security should never be permitted. The debate always starts there and escalates into a much more frightening story."

"How do you think they should protect us?"

"The way they did in the past, with evidence and brains. The problem is everyone is becoming lethargic, you can sense the complacency in almost every field. The feeling is the sense of bleakness one feels when...when you see trash on the ground at Disneyland."

"What?"

"When Disneyland was first invented they strived for perfection. You would never see trash on the ground because one of the...cast members, any one would immediately pick up every stray paper. But you can see trash on the ground at Disneyland today. Maybe cast members are looking the other way, or maybe it's someone else's job done only on rounds, or maybe there are not enough trash people. Whatever the reason, trash on the ground at Disneyland is the pop social indicator equivalent of a society facing a massive decline in effort and caring."

"When in the world did you see trash on the ground at Disneyland?"

"Don't hate. I like the rides. Now focus on the point. At every level of our society, the malaise has swept in, like a sleeping sickness. For law enforcement, an officer can sit at a desk and data mine someone's phone instead of stepping out into the streets to find clues."

"But why do things the hard way if you have technology to make you more efficient?"

"Is the technology making him more efficient? Regardless of the crime, police always jump to a suspect's mobile phone 'to see if they can find anything.' Half the time they have not even thought about the evidence to look for, they are literally just scrolling through the data as if they were trolling social media at home. The approach is not tactical, not investigatory. The police have become digital time wasters like everyone else. Law enforcement should have to think through all of the parameters of the crime and possible evidence, and only go to the phone if potential clues are pertinent to the other details connected to the case."

"I think they're finding clues to crimes."

"Sure, sometimes they are. But do they have to look at everything on your phone to find those clues?"

"I don't know, maybe."

"Their approach is too sweeping, too intrusive. The fourth amendment also says warrants must 'particularly describe' the place to be searched, and the person or things to be seized. The warrant cannot say 'we're just going to scroll through this person's online data and see what we find.' Broad, generalized flailing around in police investigations has been banned in this country for over two centuries. The liberties law enforcement takes these days are illegal. We have to guard our privacy."

"For privacy's sake?"

"For democracy's sake. Privacy is foundational to societal peace. That's why the concept is in the fourth amendment, not the 99th. We really do not need to know all the dirt on our neighbors. Privacy is also critical to individual peace. People should be able to choose the information they reveal to the world, and when or if the data will be released. The automatic assumption made by Internet companies that a person's personal information belongs to the company is unprecedented in history. When you go shopping at a brick-and-mortar store, do you expect the storeowner to follow you home and record how you use every item you bought? But online, that's exactly what's happening, and the worst part is the companies believe they are doing you a favor."

"But don't people agree to these intrusions by using the online services for free."

"All online companies, free and paid are keeping and repackaging, using and manipulating, the consumer's data. No one has agreed to this, but the practices have become standard for businesses, without transparency to their customers."

"The transparency existing now will disappear all-together with this system they plan on implementing."

"No doubt."

Dallas lowered her voice. "They're going to win, aren't they, Apex."

"No!" Apex defiantly stated. "No, never."

"But they'll get the system rolled out and you won't be able to stop the project from expanding."

"If we can't stop the initial rollout, at least we can make the subsequent build-outs difficult to implement and maintain."

"How?"

"By deciphering their exact intentions and aligning to limit the progress."

*

On the recommendation of the Secretary of State, the President of the United States prepared to sign a top-secret perpetual project directive warning all future Presidents, the COSA experiment was a national security imperative that had to supersede the vagaries of quadrennial elections. The document, to be locked in a safe with other transition materials, explained COSA's inter-connected infrastructure and the impracticability of attempting to dismantle any section of the system. The advice laid out the government and business strategy, and suggested each future President accept the inevitability of maintaining ground and online surveillance as part of the national defense against physical and cyber terrorist threats.

"But the legal implications if the public should find out..." the President of the United States stated, his concern expressed to Julia in the Oval Office on the day of the signing. Marco had joined her, as had the chairman of the military's Joint Chiefs of Staff.

"Mr. President, as I mentioned, this research project has been implemented with extraordinary cooperation. And if the experiment works, we will have demonstrated our capability to achieve the widest reach possible over the activities of terrorists."

"But we will be aggregating citizens' online activity in an attempt to predict their next move."

"Mr. President, with all due respect, on any given day there are perhaps 350 million people in this country. Can you imagine the resources we would need to really pay attention to every little motion every American, temporary resident and tourist is making each day? The conspiracy theorists can speculate all they want, but tracking every individual every minute, on cost alone, the scheme is basically impossible. This project will flag the bad guys. The system knows the difference between a gun store and a grocery store. Facial recognition is only on people we have been tracking in other systems because of their subversive activity. We don't know anything about the average American unless the person becomes a suspect. For some reason, people think we care about their every activity, but we do not. We only want the threats to our national security, and those guys come to us by virtue of their illegal behavior. They act first, not us, and definitely not the system."

"I see Justice has signed off, but I'm still not sure what the American people would think of this. Everyone is already up in arms over the cell phone monitoring mess."

"Sure but that was a functioning system implemented without the consent of the American people. This is an experiment, only R&D to understand our capabilities. We are testing the functionality and determining possible features. Once we have a concrete idea of our capabilities, we can develop a comprehensive program to formally implement for the long-term." Marco had been looking at Julia as she spoke, but dropped his head to stare at a dot on the floor as she continued to weave a less than accurate tale for the world's most powerful man. "We have to practice with the software, get rid of bugs, determine exactly the level of potential compromises, all of those sorts of tests will be analyzed before we complete the work. You really have nothing to worry about, sir. As the Justice Department said, we are only operating in public areas, there are no legal implications when people are functioning in public."

"People do not think their online activity is public."

"Only because they do not understand the fine print. The Supreme Court has already said if you hand over information to a public company to provide a service for you, like banking, that's their information not yours."

"This is different, this is about identity."

"The average person is comfortable with the process. For the life they want, a law-abiding,

normal life, they have signed up, everyone is online. Handing over personal information is not a major issue, they want to be connected and they'll want the conveniences this project will eventually deliver."

"Yes, I must say I love the opportunity to extend education through online services and help people connect their studies directly to jobs, those possibilities will be enormously beneficial."

"Yes Mr. President, the benefits of this project are fantastic. Really, if we can solidify this testing everyone will profit. We only wish to ensure future administrations understand the implications and are as insightful as you in recognizing the potential for our nation and the world."

On those words, the President broadly smiled at Julia, as he signed the paper permanently locking the system into place for the duration of its global implementation.

*

After convincing the President, Julia traveled with him to work on selling the experiment to multi-lateral organizations, while Marco took the project details to global law enforcement agencies. Beginning with his domestic colleagues who had been co-opted into COSA, but did not know the full extent of the project's implementation, he followed Julia's script and example to obtain broad consensus for an experiment which, they all assumed, had no further agenda. All law enforcement agencies were fiercely engaged in developing cyber defense solutions for presentation to governments for approval. None were particularly concerned about experimental R&D usurping their detailed, and legislated, work. As Marco ran the project details through each agency, he received indifferent feedback and limited engagement. In the range of known and unknown security organizations operating across borders, he found no objection from those interested in joining the global experiment.

After a meeting with British Intelligence, he called Julia. "No conflicts, no concerns," he told her of the British response to COSA.

"Has anyone read the details?" Julia asked.

"No. They're espousing one of those, 'we're busy putting buckets on the floor to catch the rain and have no time to fix the roof full of holes,' excuses."

"Short-term vision?"

"Exactly."

"Even with our international colleagues we are operating at the right moment in history."

"Yes as I go through these global meetings I realize the winds are blowing in our favor. No country has world-defying leadership. We have a strength and courage vacuum, that's why terrorists are going for destruction with impunity. They do not see the galvanizing of global forces prepared to destroy them. But when we talk about COSA, everyone is ready for exactly this type of response."

"Because we can't find the terrorists. But COSA will."

"Maybe we could find them if we had the people. But the discontent is everywhere Julia, like dust. All of the global law enforcement agencies know they must be able to answer questions about cyber security. They prepare their people and the work to meet the challenge as a technology issue. But our plan is different, we are not only looking at protecting computer systems. Our version of cyber security includes using cyber to ensure security. We're investing for the long-term in a comprehensive system, but our counterparts do not have the vision or the money to pursue that option. At the same time, there is an extraordinary amount of money available in the world. Taxes are generally low in most developed countries or tax loopholes are high. Real assets of value like real estate, artwork and jewelry are increasing in price at a rate

consistently exceeding inflation. China is only part of the story, the rest of Asia, the Middle East, Africa, there is new wealth everywhere. And we have access to these growing financial funds. Someone can afford to buy at those prices, and those people can afford to invest in their own cyber infrastructure. In a way, I cannot believe our luck to have this project success at this point in history."

"We have worked very hard to get to this point. Luck is opportunity meeting preparation, my friend. Do not discount our individual efforts."

"No, no of course not. But we have this unprecedented world situation of feckless non-cooperation in Washington, inert global capitals, multi-billion dollar wealth funds..."

"Don't forget the media. True investigative journalism is dead. The media companies are giant conglomerates focused on a bottom-line aimed at generating advertising dollars by capturing eyeballs. I would bet the average reporter is some social-media-addicted college kid who has no idea of the role of a traditional newspaper journalist to go out and research and investigate, and to provide readers with uncovered insight into vital stories."

"They certainly write that way."

"The news media has reacted to social media in exactly the opposite fashion one would have expected from traditional journalists. They follow social media around for stories, instead of going out and finding and making news with their own curiosity."

"Sad."

"Yes it is. Your friend Dallas could have been a journalist from another era but even she was intimidated into dropping the story. Back in the day, she would have taken a risk to make sure the public was informed."

"In her defense, we made the story impossible to find. She would have looked like a fool if she tried to write about a grand conspiracy to take everyone's personal data."

"But she would have been right."

"Except no one would have known until after she was dead."

"No one will ever know even after we're all dead."

"You think this story will never leak out."

"What's to leak? A recording of this conversation?"

"No, not today, but only because we assume our technology is superior to the plans and ideas of those who will seek to bring this system down."

"Who?"

"You know, the hackers."

"The hackers do not have a cohesive idea of our plans."

"But as the project is rolled out, as the system becomes public information one day, the hackers will realize what has happened and take their revenge."

"They'll be too late."

"With technology, you cannot be too late if you have the brainpower and time to push further ahead."

"We'll have to keep them from pushing ahead."

"How will we prevent an inevitable quest to attack us?"

"By staying on top of the information they think they have."

"Planting deceptive stories?"

"Maybe."

"Or a completely deceptive system?"

"Possibly."

"You're going to camouflage COSA?"

"Of course. The system cannot be an open website one logs in to. We have to make sure the connections are untraceable, tied behind other systems and locked through inaccessible doors."

"But eventually the project will encompass all of those other systems and other doors."

"Yes but at that point, the whole world will be connected through their smartphones and every other electronic device in their house and workplace. At that point, people will be so dependent on the functionality one will not be able to sabotage the software or servers because of the potential to destroy whole swathes of society like airports, schools and hospitals. Once everyone around the world is on COSA, the hackers will have no scope for attacking. They would shut themselves down too, lose electricity, water, even contact with each other. Mutually assured destruction is still a deterrent."

"Yes okay, but only if they have no insight today, as we want to believe."

"If they have any information, the details will not be enough to stop us. On that I am completely certain."

*

Julia's rollout of the COSA experiment to world leaders at the G8 and NATO summits was equally flawless. With the President as the project's unwitting champion, Julia placed him in front of his colleagues to quietly proclaim his excitement over the project and its potential. For those expressing reluctance, Julia prodded the President to remind them the project was 'in test phases,' and the research was required in the name of global security.

On the sidelines, she exerted her own additional words of influence.

"*Monsieur le Président*," Julia said, waylaying the French President during a dinner party at the G8. "You of all world leaders know this project is a crucial step in the fight against terrorism. Your support will encourage your government and businesses to participate. That's all that's required at this stage, participation."

To the British Prime Minister she emphasized the value of interconnected functions and early alerts about border-crossing hackers.

Both leaders agreed.

At the NATO Summit, smaller countries were eagerly overwhelmed given every major country appeared informed, enthusiastic, and prepared to engage and share in the results of the project's functionality and potential. As Julia told the Baltic and Scandinavian nations, "Participating is straightforward. You will want to learn how well the software works. You do not want to be left behind on technological developments. At the least you will have a front-row seat to the latest innovations and capabilities of advanced surveillance technology. Really in this day and age, you can never be too careful. You should at least know which tools are available in the event of a real fight."

By the time she completed her rounds, all 28 member states unanimously agreed the need to have a global surveillance approach to fight terrorism required an advanced interconnected global technology solution, and all committed their governments to joining the COSA framework within the year, and to participate in the experiment and analysis of the tracking results.

On the final night of the summit, Julia called Marco. "I will see you next at *Eglwys Gadeiriol Tyddewi*," she said with a hint of humor.

"Where?"

"We are meeting there, in the Library."

"The library? What library?"

"In *Eglwys Gadeiriol Tyddewi*."

"Those are not even words."

"Don't be such a nativist, get into the spirit of the location."

"Where am I going?"

She laughed. "To St. David's in Wales."

"Wales? And this mysterious unpronounceable place you apparently mentioned?"

"The Cathedral."

"The Cathedral? The library in the Cathedral in St. David's in Wales, sounds like a 'clue-risk' marriage gone wrong. Could there be a more obscure location?"

"Another uninformed comment. St. David's is not obscure at all. It's a perfect place for us to go, but not readily accessible to our potential followers. Bring reading for the haul from Cardiff. I'll see you tomorrow."

"Okay, " Marco reluctantly agreed.

The narrow roads of Wales cut through the low hills and lush green flatlands as thin pencil lines tracing the outlines of clouds floating in the sky. Every twist brought a renewed view of the territory jutting out from the west of England into the Irish Sea. Having snuck away from the NATO Summit's delegates' hotel before sunrise, Julia caught the unobstructed crisp scent of a waking day and failed to doze as planned, as her private car carried her across the length of the territory to the tip of the peninsula and settlement named for the Welsh people's patron saint, David. With Tudor perfection the restaurants, pubs and shops of a village insisting on being called a city, emerged in front of Julia as if stepping out of the postcard describing its medieval beginnings. 'The U.K. never disappoints in its maniacal commitment to the past,' Julia thought, as the car moved on towards the reconstructed stonewalls on the 1,500-year-old cathedral grounds. Despite an ends-of-the-earth location with no rapid transportation options, St. David's dared pilgrims to find its hollowed ground as the satisfying finish to an inconvenient journey. But here, Julia and her GCS group would be lost to the official media covering the summit more than one hundred miles away. Instead her colleagues would be incorporated among the pious and the curious who would assume, like them, the trip had been made only to take account of the historian's and the believer's confidence in its importance. Disembarking on arrival, she made her way to the Cathedral Library, which had been privately closed, and joined her global GCS team ready to celebrate their victory in persuasion.

"Congratulations," were the first words to greet Julia as she shook hands with the meeting participants, those who had been at the G8 or NATO summits did not need a recap of her ability to obtain cooperation for the global rollout of COSA. Within a half hour Marco and all the others arrived for their first and possibly last in-person meeting as GCS.

"What we have achieved around the world is remarkable," Julia stated, addressing the entire group. "You have all done an excellent job. COSA has been established for the long term, for the future we want to see happen. Within the next ten years, Western governments, many businesses, universities, and law enforcement will be connected, and we will be able to see the profiles of millions of citizens. As each year goes by, we will extend the functionality until the foundation is completely unseen. In the future, the average person will use COSA to go about their daily business as if the system's commands were a voice in their head. We should catch every terrorist before he acts. COSA cameras and sensors will always know when danger is near and law enforcement will be immediately alerted. This ability to use technology to change human behavior is the 21st century equivalent to the domestication of animals, the cultivation of

crops, building a public school system, inoculations..." She laughed. "You get the point. We have single-handily set-up the best law enforcement tool the world could have, and we accomplished our goal without government interference or public protest. If people ever get to the point of complaining, which I do not believe they will, another story will rapidly be told about how the benefits of this system improved the lives of millions...billions of people. We may not have the opportunity to be publically congratulated for the work we have done, but we will know and celebrate our achievement among ourselves. In places like this remarkable cathedral, surrounded by beauty, arts, culture, spiritual guidance and history...we will celebrate and remind ourselves of the incredible pinnacle we have reached.

I thank you all again for your hard work, cooperation and incredible courage in the service of humankind. We go forward, equally vigilant against our enemies, against those who may seek to disrupt our work, and against those who do not understand the value we are providing by using technology to these ends. We will have to fight them, we will have to be more organized and committed to our project. But we have the advantage of already being implemented, of being in place and ready to be used by the populace. Our enemies, whoever they are, cannot be much more than a misled bunch of anarchists who will haphazardly approach us in disruptive battles. But we will be ready for them. And we will win."

At the conclusion of her words, those in the room ignored the mandated decorum of the scene and jumped to their feet as they broke out in prolonged applause. Julia nodded to each in turn, a smile of contentment and gratification etched on her face as she took the moment to stand unchallenged in a world made accessible through one light touch of a finger to an icon on a screen.

*

At her home office, Apex carefully read the detailed COSA overview file prepared for the President of the United States' trips to the summits. FedSec explained the project as a spontaneously created database integration by concerned businesses and agencies, and recommended the President support all government departments' participation in the global experiment. 'What a bunch of liars,' Apex thought. 'Some experiment.' The document did not call for Presidential or any other level of approval. Instead the experiment would be rolled out as a test, and miraculously over the years no one would bother to roll the system back. FedSec's careful language did not bind the administration, nor government departments, nor industries, yet within a couple of decades, the organization expected the early phases of the project to be flawlessly functioning for global surveillance tracking integrated with personal online data.

'Carter was right,' Apex conceded. 'They have set up an entire global system to move forward without human intervention. No government department has a reason to withdraw from an experiment aiding national security. The funding from each department is minimal, no one can see the underlying financing located all over the world provided by those who expect to benefit from the data aggregation capabilities. No one has a view into the entire picture of this project, its mandate is to take personal privacy and hand the data over to governments and businesses. There's no story for the press, no obvious crime against which the public could rally. Only a carefully thought through scheme designed to provide a window into private activity for a government bent on control.'

But Apex knew there were people who would take the time to analyze the details and would be able to understand its implications. Diligently, she prepared a summary of the document's key points - the planned connection of the project's server farm infrastructure and the intentions of its consumer facing views. Packaging the summary with the original blueprint, she e-mailed the

files to every independent technologist she knew, everywhere in the world.

*

For businesspeople, scientists and academics, Carter began his promotion of COSA as surreptitiously as possible. Beginning with close friends who were the founder-owners of consumer facing technology companies, he privately spoke to them about the long-term efficiencies to be gained by cross-referencing all user data across multiple websites. No one was skeptical about the benefits, all questioned the legality, or more importantly, consumer acceptance. Carter repeated the claim that the rollout was only a test, and businesses could build a separate database, mirroring the existing one, but to be used only for research.

"Believe me no one is more torn about this turn of events than I am, " Carter told five friends at dinner in a secluded restaurant in Tiburon, California, across the Golden Gate channel from San Francisco. "My contribution could turn out to be the worst thing I have ever done. But if I never see another terrorist incident, maybe my work was the best thing. Either way my motives here begin and end with the technology. Regardless of how the functionality is used, we have to know our ultimate capabilities. People who have worked on this project are stunned by the results. We are next gen leading the way on facial and body movement recognition. This functionality can be used to find missing children or seniors with Alzheimer's, not just wanted criminals. The extended reach into everyday life is even more profound. Think of a world where routine tasks are just done, completely automated. I'm one of these people who hate doing administrative chores...you know going to the DMV, registering to vote, buying insurance. In future phases, all the time standing in line and filling out forms will disappear. My health care premiums will be directly tied to my actual health, the food I eat, even the environment where I live. Drones can deliver my groceries or carry my bags from an airport carousel directly to my house? Don't you want to be able to have all of today's wasted time to do things you really enjoy?

And education. We should not be losing a single child, or even adults because of a lack of education. Kids should have a learning program tailored only for their personal needs. I was also thinking about at-risk kids, boys in gangs, what if we could get them to sit down at the computer for a few hours a day and have all of the lessons built around the factors in their life. We could prepare lessons around the subjects they are interested in. So for example an African-American gang kid could come to a safe place, sit down with his laptop, do an hour of writing practice using only the histories of successful black men as teaching tools, and we've got him. Next time it's two hours and his science lesson is about how compounds join to create drugs, pharmaceuticals, not illegal drugs. Maybe he'll stay for a third hour to do math lessons if the examples refer to objects in his neighborhood. Think about the value of that kind of personalized education. The average kid spends more than 10,000 hours at public school. We could ensure the same level of learning in half that time, and add additional layers of tactical studies aimed at preparation for the job market. The impact on our nation would be tremendous.

So I admit, I'm excited by the opportunity to provide every citizen with a uniquely directed life. We'll be able to better manage transportation, electricity, water, waste...think about getting rid of landfills, and this state's water shortages. The potential is enormous and exciting. But the question is 'should the government know everything about you?' My answer is 'no' and the system will be fully equipped to let you opt-out. Of course, from day one you'll be opted-in so by the time someone is an adult and aware of the extent of gathered information, effective opting out will only be on a go-forward basis. But the functions will be available. Opting-out as an adult may also trigger law enforcement to think you've gone off the grid to join subversives. But

the camera and sensor surveillance will cover you. The government will still see you operating in public places so no one will bother you if you decide you do not need a daily life update from the system.

Look, I know we have a fine line here, but the potential and the opportunity are fantastic. We are missing a lot of people, under this system we won't miss anybody. Governments will have no excuse for ignoring the homeless or pretending education and job creation are working. There will be live, real-time, exact statistics available every second on unemployment, affordable housing, education levels, food consumption, transit use, everything. People will have total transparency around taxes and spending...I could go on and on."

"Don't bother, Carter," one of his friends protested. "You're a total sell-out. You've got to be out of your mind to be promoting this system. This idea is a gross invasion of privacy. I'm not signing my company up for a government experiment to implement Big Brother everywhere."

"Let's not be alarmist," Carter calmly responded. "This is one of those moments when you have to pick a side in history. Technology, our technology is here to stay, but do we let governments determine how and where they want to use our innovations? Do you want a seat at the table or not? At the end of the day the system works best when everyone has opted in, but stays alert to how to participate. You don't want a situation where you cannot attract employees because they want to run their lives online and your company is still requiring them to do all of the company's work and administrative tasks in a separate system. Don't worry about security. I know that's the other big concern. Your intellectual property can remain behind proprietary digital locks and keys. But this system is about your employees being able to manage their lives online. You'll want to connect employment access, healthcare and retirement plan information and maybe extras like parking passes and daycare clearances. Why would anyone want to separately deal with each of those issues when data from one could feed the other? The better connectivity you have, the easier the rollout will be for your employees.

But remember at the end of the day, how you manage your life online will be up to you. Education and awareness will be the keys to making sure this system is a benefit and not a subversive burden on the average person. And we have the responsibility to define those options. We are the professionals who understand exactly how this project is expected to work. We own this technology. We also have the world's best technologists working with us. At the end of the day, no government will be able to make the system function without our help. We will be the monitors, the guardians of our consumers' privacy, and we can control the technical operations, as we want. If you sign on now, you're making the decisions. The results of these tests will be the framework for an eventual fully global system. You do not even have to update your test server environment because the data could be static until such time as you realize the benefits of the plan. Really we, the technology industry, we hold all the cards here. You can sign up, check the system out and make a decision, your decision." Glancing from face to face across the table, he said with finality, "I hope I've addressed all of your concerns."

For better or for worse, he had.

With Carter's caveats and assurances, more businesses signed on. Holding tight to the option to opt-out or to change the parameters of their involvement, and to maintain at all times the right to manage their own consumers' data; participants provided the COSA team with access to their servers in exchange for the test results and the software.

Privacy advocates, who learned of the project's existence through managers and executives in business, had no recourse against an unofficial, experimental process no government legislated

into law. Concerned activists complained to the media to report that the foundation was being laid for a permanent system, but few believed their warnings. With each tentacle reach from one server farm to another, more outsiders wanted to be in, and the opportunity to grow the experiment expanded exponentially, beyond even the original estimates calculated by Julia's team for the first few years of the project plan.

Test results were disseminated to all participants and the value they saw was astounding. Aggregated data was used to create an individual's profile in which a business or government could view a range of activity, not only expected shopping, banking, traveling and social media habits but also the location, demographic, frequency and quantity data needed to predict behavior. Where available, COSA cross-referenced surveillance data and added the individual's non-online activities into the profile to obtain a complete picture.

Participants began exchanging information about the findings, and those conversations were recorded in e-mails intercepted and read by Apex and her friends as they diligently, and patiently, established their foundation for fighting back.

But as enthusiasm grew, so did traffic about the project and its possibilities. The satisfaction continued to extend around the world. When global governments began to recognize the permanence of COSA, they realized the system would need a permanent home, organization, and more palatable name. After intense discussions centered on issues of national sovereignty, the world's governments agreed to allow the United Nations Security Council to establish a unit for cyber security incorporating COSA and its future development. To avoid a controversial tone of permanency, the Council called the group, Special Command for Cyber Security, established its headquarters with the U.N. in New York City and appointed its head of operations who was initially given the title, Director.

Within the U.N.'s budget Special Command's funding was limited to the surveillance equipment infrastructure, real-time feeds from all cameras and sensors set-up around the world and satellites the organization could access through its own links, and the data aggregation software to aggregate all of the information, as well as the daily operational costs of salaries and administrative overhead. But unofficially, GCS established a permanent funding organization to provide Special Command with additional resources whenever a global issue needed to be resolved without the constraints of the U.N. budget process.

As COSA's original name had proposed, the project became complete online and surveillance aggregation, every step and action each individual human took was recorded as a life online. The original system uniting all of the proposed functionality evolved into popular use, accessed from mobile and static devices and openly referred to by civilians and governments alike by a much more evident name, The Network.

*

EPILOGUE

One hundred years later...

The alarm buzzed inside Louis Santino's apartment at 6:37 am. Santino had not set the alarm as humans had to do in the past. The Network automatically calculated his wake-up time

based on data stored in his individual profile. Using his expected commute time including adjustments for real-time weather or traffic conditions; the amount of time he took for breakfast; and his grooming and morning exercise routine, The Network determined how many minutes he would take from rising out of bed to arriving at work.

Picking up his com, a palm-sized, flat-screen plastic electronic device the size of a playing card with a velcro-like adhesive attachable to any type of clothing, Santino fell back onto the bed to view his daily schedule. All communication devices, or electronic tools with similar features, were called a com, the abbreviated term replacing a range of recognizable words like phone, radio, television, camera, or personal electronic device. Although a com could be any size or shape, and manufactured to operate within almost any device, all had one shared function, wireless connectivity to The Network. After selecting an icon on the device, a daily calendar image opened as a transparent screen suspended in the air in front of Santino's eyes and displayed his activities for the day. Santino rarely checked his schedule, but the action was a convenient delay tactic to avoid instantly getting out of bed.

His schedule was automatically adjusted and updated using factors from his life, work and habits. The Network accounted for every minute of Santino's day except bathroom breaks. No technology had yet been developed to predict exactly when an individual would require a bowel movement. Although Santino looked at the activities on his schedule, his gesture bordered on indifference, he would not be deviating from any instruction sent by The Network, he never had. Standing up, he performed a few quick stretching exercises and went to the bathroom. In the shower, he selected the 'water on' button. The Network had warmed the water to his desired temperature and when the stream came out, the nozzle provided exactly the pulse and intensity he desired before automatically shutting off to allow him to soap up. He hit 'on' again when he was ready to rinse off. By holding down the button for an extra three seconds, he could override the automatic water conservation features. Santino lived in northern Canada where water shortages were not an issue. In the southern U.S. states, prolonged drought forced people to ration water supplies, and water-control showers were mandatory in every installation. In those areas, The Network maintained control over how long water ran during each shower use.

The Network had several other manual overrides and options for humans to retake control of activities the system was programmed to manage. But most humans accepted defaulted commands for their life actions. With the exception of profoundly underdeveloped areas, every human born on earth, or in outer space, received a Network profile with the generation of a birth certificate. From that day forward, The Network populated the profile with data about the individual and used the data to generate life instructions for those willing to accept the convenience. The Network continuously scanned servers, even those not exposed to the public Internet to retrieve, cross-reference, and integrate data inputted as official government records, generated education results, consultations, food consumption, text and voice communications, videos and photos, and employment reports. In public areas, recorded movements from cameras and sensors tracking all manner of human activity were also automatically stored on servers, and retrieved when facial recognition and body movement software was used to identify suspicious individuals. The mass of data files was aggregated through a variety of government or business software applications to create and send appropriate daily life instructions, specifically prepared for each individual's com. The Network provided access to millions of programs and applications designed to continuously repurpose data to feed a human's com, and the human reacted accordingly.

Santino dried off, dressed and wandered towards the kitchen. He lived alone in a one-

bedroom apartment in one of the few mid-sized high-rises built along the main road in the small hydroelectric power station town of Grand Rapids. In major cities, population densities prompted urban planners to build all spaces vertically, and the population lived, worked and played within inter-connected high-rises. But small towns maintained separate buildings unconnected by tunnels or subways or people movers or mass transit stations. Santino could look out his window and see rows of bungalows and two-story houses with driveways and backyards. In the cities, only the wealthy and the highest-paid professionals lived in individual family houses in suburban residential areas. No one else could afford the maintenance costs for private utilities that the neighborhoods had to pay to remain connected to The Network controlled electricity, water and sanitation systems. Approaching his mid-forties, Santino would have preferred to be in a house, he enjoyed the idea of space and access to private land. But he was hoping to find a wife first, and move into a house with children. Most days, he devoted a few hours to online dating. But although women enjoyed speaking with him, they were reluctant to travel to a small town in the cold Canadian north to spend time with a man, when the amusements and options in the city were readily accessible. Still he hoped one day he could entice a woman to at least visit him. If only he could convince a woman to make the trip, he could demonstrate his ability to offer a family a comfortable life, including vacations in warm weather locations, and all the amenities and conveniences available in advanced societies.

Maybe this weekend he would receive a positive response, Santino thought as he entered the kitchen. Lights illuminated and the coffee maker automatically began brewing when he passed by sensors in the doorframe at the kitchen's entryway, which cross-referenced his presence to the time of day. From his fridge, he extracted two eggs, bread, butter, and orange juice. He preferred his own cooking to the processed options available to order online or buy in a store, especially since The Network monitored eating as part of creating health alerts. The system cross-referenced the food items with his medical records and recommended changes if his vital signs showed any signs of stress. But too many alerts led to an increase in health insurance premiums, which healthy people always tried to avoid. A sensor recorded the items removed and replaced from the fridge, and an electronic grocery list on the fridge door flashed a message if any product was running low. A similar list appeared on his pantry door. Santino could add or delete items as desired, but he never actually read the grocery list. His fridge was never empty, he never went grocery shopping, and he was never without his preferred food on any given day. The grocery lists indicated the current amount of each item and noted when replenishment items would be automatically ordered for delivery by a commercial drone. The kitchen list information was connected to the closest grocery store, which delivered replenishments when necessary, without prompting.

Along with the lights, a monitor screen had lit up and was displaying the broadcast from a sports channel. Santino listened to the commenters talking about football. Today was Sunday and he would have professional games on all day while at work. Another screen was projected above the sports, and displayed the temperature and news headlines. Trying to remain engaged with the broader world, Santino checked news every morning to ensure he was not missing any important world events. In general, he was interested in other regions still experiencing civil unrest or threats from hostile neighbors or violent crime. These stories were always intriguing since global surveillance using cameras and sensors made criminal activity difficult to plan and execute outside the vision of official electronic eyes. Still, a large segment of the population, more than the government cared to admit, were diligently working to avoid The Network. Some were vocal and public about their activities, living in rural towns and remote areas and

encouraging the broader populace to join them; others were hiding from law enforcement or seeking to sabotage The Network's control of personal information. Santino was never really sure what to make of these people. He could not imagine functioning without The Network, the whole world ran on the inter-connection of electronic devices. Still he sometimes felt he should do more on his own volition, but often he could not imagine exactly what 'more' would mean.

Besides the international news, he glanced at domestic headlines, but he was less engaged in the pronouncements of governments who claimed to have appealing ideas aimed at creating a more productive life. The national government used The Network to set policies and to calculate taxes to pay for announced plans. Since The Network could predict government revenues to the minute, taxpayers fought for stricter fiscal spending and less debt. Depending on the administration, the response was action or indifference. Either way, Santino avoided listening to government excuses. His life, he determined, was sufficient, although not ideal, but the missing pieces were hardly the purview of any government to satisfy, at least not yet.

Finishing breakfast, he placed his dishes in the dishwasher. The machine determined the capacity, but did not start since a cycle had run two days earlier and the pieces inside were not enough to indicate Santino would soon run out of clean dishes. As he walked out of the kitchen, the coffee, lights and TV monitor turned off. With his com attached to a strap on his belt, he took a look in the mirror and walked out. The Network locked his door and turned down the heat in his apartment.

Arriving in the lobby of his apartment building, Santino greeted his neighbors who were waiting for their transports, driverless vehicles with the functionality to hover through the air forward, backward and sideways, or to move with wheels on bare floor, carpet, gravel, grass, cement, ice, snow and heated terrain. Through the building's glass front doors, Santino could see the snow and ice covering the town's landscape, but neither he nor any of his neighbors wore coats, boots or other cold weather gear. Instead they waited as each transport came directly to the door. Since only one transport could fit in the lobby's vestibule at a time, they patiently allowed each other to proceed in the order of the transport's arrival. Humans owned personal transports or hired the vehicles on a usage basis. Either way each trip was programmed and automatically controlled via The Network and average commute times were calculated for each distance traveled, for every trip ever taken. The Network would also know weather and traffic conditions for the day. Despite transports' flying flexibility, to avoid disturbing people in their residences or disrupting the tranquility of parks and public areas, all vehicles were programmed to travel on or above the routes laid out by paved roads. No significant traffic congestion resulted from this directive, transports automatically adjusted to other vehicles, drones, birds, and other objects in the air, to avoid collisions. However speed concessions were made when more flying entities were moving at the same time, and snow or heavy rain could interfere with the controls and force slower, more cautious routings.

Santino traveled to work in his own private transport, which permitted him to keep the vehicle stocked with his favorite drinks and snacks. On arrival, the lobby door opened at the same time the transport door opened and he climbed in without feeling a blast of cold air. As the transport door closed, the vehicle's sensors read data from Santino's com, and a monitor screen popped up to display the same sports channel he had been viewing over breakfast. He reclined in his chair, which was set to his height and comfort levels, and lay back to watch the show as the vehicle rose off the ground and pointed in the direction of his workplace.

Less than half of the employed population physically went to work each day, but Santino was a technician in the hydroelectric power station. His job, which was to monitor the

operations for issues, required his presence inside the facility. Built at the top of two lakes in Manitoba, a province in the middle of Canada, the power station was one point of a multi-billion dollar interlocking grid of clean energy plants, reservoirs, sub-stations, and thousands of miles of transmission lines stretching across North and Central America for 6,000 miles from the Arctic mining towns at the furthest northern end to south of the Panama Canal. The grid was a significant source of electrical power for a dependent population of over seven hundred million people, and a vital distributor of water for the agricultural centers of the continent. To ensure continuous production, the Grand Rapids complex had more than 10,000 cameras and sensors, dozens of operational drones, and one human employee on site per shift.

Upon arrival at the plant, a garage-like door automatically opened as the transport carried Santino into the facility. The departing overnight employee was already waiting inside his own transport to leave as soon as Santino arrived. His colleague immediately passed by with a brief nod of greeting before the garage door rolled back down again. Santino climbed out of the transport. Sensors registered his arrival by locking on the signal from his com. The Network automatically noted his arrival time, which was within three minutes of the time determined from the moment Santino had woken up at the sound of his alarm.

He walked into the control room and glanced around. All data and sensor readings were green. No issues were reported. Santino felt obligated to do his initial glance around even though he had never had an issue reported in his sixteen years on the job. The employee personal monitor screen turned on to his sports channel, and Santino settled in to his chair for the day. A drone flew into the room with a cup of coffee, its grasping claws carefully placed the steaming mug in the cupholder on the armrest of Santino's chair, not a drop was spilled as the cup handle was turned in towards Santino's hand. He took a sip and focused on the screen.

After two hours, Santino's com beeped, he had a mandated walk around inside one of the facility's server rooms. There was no issue in the server room, but government healthcare regulations prompted The Network to schedule exercise for employees who might otherwise be sedentary throughout an entire shift. Projecting a screen from his com to continue watching his sports entertainment as he walked, Santino noted the message stating he was required to remain moving for twenty minutes. Since he completely disliked voice commands, The Network projected a step-by-step directional guide for Santino to follow while the com registered his movement and The Network recorded his compliance. If Santino did not complete the walk, The Network would note his deviation and his health insurance premiums would be adjusted to reflect his lack of exercise. If he substituted the walk with separate exercise at a local gym, the adjustment would be made again. To have a run in the open-air count on the medical records, he would have his com monitor his heart rate and send the workout report to his medical file. But Santino did not run in the open air, especially in winter months, his mandated workday walks, and morning stretches, were the only exercise he actively undertook.

With no specific task to complete inside the server room, except to keep walking as his directed workout, he completed the round within the twenty-minute timeframe and returned to the Control Room. Arriving back, he dropped into his chair. When a live football game featuring his preferred team began, the monitor automatically switched channels and displayed the game broadcast. Santino had not moved from his chair. But he knew after two hours another walk alert would appear, and he would once again project a screen from his com to keep watching the game as he moved around.

At mid-day, a drone flew into the room carrying a miniature-heated oven, about twice the size of a lunchbox, and run on battery power. The drone placed the oven on the table in front of

Santino and used its long pincer claws to place a hot meal - a burrito, tortilla chips and a soft drink - on the table before him. When he had first moved to Grand Rapids, Santino had manually ordered lunch from every nearby restaurant with delivery options to the hydro station. After selecting his favorites, he had programmed the preferences into his com, and every workday a delivery message was automatically sent to the next restaurant selection on his list to bring his lunch at a scheduled time and charge the cost to his credit account. Since the drone was pre-cleared for delivery, the facility's doors automatically opened when the machine arrived and projected an admittance request message at the entryway sensors. The programming also directed the drone to the control room and pinpointed the table where the meal should be placed. Santino was feeling hungry and had expected the meal to arrive at any moment. When the drone completed the meal set-up, he did not take his eyes off the game, but mechanically moved towards the table and began to eat.

When Santino had finished eating, he selected the cleanup icon on his employee monitor. A robot appeared holding a trashcan in one metal hand. The machine was made from refurbished steel and built to resemble a human with two legs and two arms but with a monitor screen head displaying text messages. Proceeding directly to the table, the robot used one mechanical hand to pick up all of the paper and leftover trash and placed the items in the trashcan. Santino was not exactly aware of the robot's next movements but he knew the machine carried the trash to a waste disposal station where sensors separated all material for recycling as paper, plastic, food or other waste. As the robot departed, Santino settled back across his chair once again.

Santino's daily routine was also his life. The Network required no thinking, no additional input, no pro-action, and no consent. Around the world, billions of people employed in programmed jobs or staying around their homes, were stepping through their day based solely on instructions coming from The Network, with no awareness or consciousness of how they had arrived at this point. The system had always been there, as a protector and guide whose primary singular purpose was security, but whose primary singular functionality had become, human control.

Late in the afternoon of Santino's routine day, generation of data inside The Network would ignite a physical reaction, a fire, burning inside a data cord in a server room at the hydro station facility. Initially no human, machine or Network action would respond.

The careful, relentless Network programming designed to identify every anomaly in electronic operations would pause.

The human selected by evolution to operate by virtue of a thinking brain, at an advanced level over all other species, would be inert.

The machines requiring either a human or a networked-system to operate would be immobile.

With the exception of the background noise of the football game, silence would continue throughout the facility. But unlike a human who can decide to stop moving, The Network's mandate was to continue functioning on a faultless, inflexible schedule of productivity. A machine programmed to action, reacts. And unknown to an unwilling Santino and an unaware world, The Network's response would push humanity beyond all habitual routine, as the first signal was received that the humans and The Network had begun to diverge from their shared point of origin.

###

Life Online is just beginning...

Read the bonus excerpt Chapter One of The Motion Clue to find out what happens next with Santino and the unexpected disruption to his routine day.

Learn more from The Origin Point story by reading selected redacted documents from the Contents on the Mystery Flash Drive.

Find much more about the Life Online series at Case Lane's website.

THE CONTENTS ON THE MYSTERY FLASH DRIVE

A Note from Dallas Winter

In the early morning hours of Easter Sunday in 2014, I was given a USB flash drive containing documents I believe where created by the United States Federal Security Commission, known as FedSec. These documents outlined a detailed strategy to create an online system for tracking every individual on earth. The documents were classified TOP SECRET. I am not permitted to reveal any details including the names of participants, the physical locations of server farms and other information about the foundational origins of the system, which would eventually be called The Network. To be fair, out of context, the entire set of documents has too much detail for general release.

But to provide you with an idea of the issues we will be dealing with as a society, I can release a one-page summary of selected topics that essentially captures the concept proposed in the document. It is hoped that releasing these summaries will generate discussion about the issues, and the legal and policy implications for the future.

DISCRIMINATION

Preventing the next Dr. King or Ms. Steinem from Gaining a Foothold: Hiding Race and Gender Bias in Website Code

THE ISSUE: *Businesses will be able to program race and gender discrimination into the software code of websites, preventing targeted groups from obtaining a product or service, or a fair price.*

Hanging a "Whites Only" sign outside of your business is likely to generate the wrath of civil rights groups, the immediate reaction of law enforcement flying the flag of the 14th amendment, and no end of taunting from local teenagers. The local Better Business Bureau will know to disown you, and what few patrons that remain will only gingerly offer support, usually behind the barrel of a shotgun.

But if you code "Whites Only" into the software code of your business' website, you may be

able to circumvent all of this unrest with no pushback.

The decision of Internet companies, retailers and other organizations to collect online personal data that can be used to create individual profiles, may lead to the creation of cyber Jim Crow for businesses that want to carefully manage their clientele. This not only applies to traditional bias along race and gender lines, but also discrimination by profession, zip code, education and every other factor that is being secretly collected by entities that consumers do not know.

Businesses are already in a position to readjust rates and prices based on selected factors. Creating another level of adjustment for the consumer's demographics would not be a difficult leap. A resort hotel trying to avoid journalists could code "no vacancy" when a user with that profession attempts to make a reservation. A business looking to encourage an affluent, youthful clientele could provide limited customer service when an undesirable age or zip code makes an inquiry. The question is – how would you avoid getting caught?

In the past, a person would try and rent an apartment, which is available when calling about it, and then rented as soon as the landlord sees the prospective tenant. The prospective tenant would send a different demographic friend to try the same approach, and document the results. In the cyber world, where data is updated second by second, consumers would find it difficult to prove that a "no vacancy" at a particular point in time was only directed at one user. Complainants would have to subpoena the offending code, and have the program deciphered to prove that it was set-up to avoid specific groups. Right after an allegation, a business could easily replace or re-program the code, removing any trace of suspect software. A consumer would have a difficult time conclusively detecting discrimination, and making a valid claim.

The real issue for consumers is that Internet companies have made these practices possible by collecting and distributing personal information, without transparent standards. This action, by itself, has opened the door for the future civil rights violators.

THE PROBABILITY: Easy to do and difficult to prove, the current competitive marketplace may only be delaying what businesses could determine is an acceptable risk.

EDUCATION

Happy 4th Birthday, Please report to a computer: Requiring an Online-Only Education

THE ISSUE: *The entire school curriculum for a one-hundred percent online education could be made available as a complete alternative to attending traditional school. The goals would be to end childhood stress from bullying and teacher complacency and bias, and to save billions of dollars.*

What is an education? It is a process used to provide a human with basic skills such as reading and writing required for operating in a modern civilization, and a common basis of information that can be used as a foundation for future knowledge. Whether the objective is spread out over 2,500 leisurely days, or crammed into half that time, hardly makes any difference to the child's

eventual standing as an adult who has retained the information. If the process could be completed without the organizational, social and logistical headaches of forcing every child through a common school system, it may end up improving focus, accelerating learning, instantly updating to changing labor demands, and saving billions in one sweep of a keyboard.

Access would begin as soon as a child turns four years old, when parents receive notification that an account has been established for the child in the public school education online system. The entire curriculum from pre-K to Grade 12 plus advanced placement courses would be made available, complete with lectures, books, tests, exercises and a suggested study schedule. There would be no set school year, no defined beginning or end time. Parents could schedule the school day exactly against the hours of their own working and commuting time, and continue through the summer or other holidays based on the family's vacation plans. In most communities, children would report to a study hall where monitors would patrol the cubicles. Each child would be scanned in, and all online time would be recorded. Cameras in common areas would record all activity. Breaks would be programmed based on the student's pace of work, for example every 90 minutes. Students could test out of material they already know, and accelerate towards completion long before their 18th birthday. They could also complete college-level coursework, removing one or two years of higher education loans from their future.

To ensure compliance, students would be required to report for testing at their current level, every 90 days, and if they fail to achieve a passing grade they would have to report to a traditional teaching environment for at least one year. Even if only half the children in the country have the discipline to succeed in this system, the resources that would be saved would be enormous.

For socializing, existing recreation centers and school buildings could be used to continue with sports, music, arts, drama, leadership and other extra-curricular activities. But these would be organized and managed by parents, professional coaches or expert instructors, and other interested citizens which would have the added effect of ending a reliance on teachers as babysitters, and improving the community's level of engagement with children.

THE PROBABILITY: While the basic curriculum is already available for home schooling, the next step will be the creation of advanced online tools, and whole communities demanding the transition away from their traditional, failing school.

LAW ENFORCEMENT

No License to Kill: Civilian law enforcement protocols for armed drones

THE ISSUE: *Law enforcement drones equipped with cameras and sensors are used to patrol urban areas. All are weaponized, programmed with automatic disarmament protocols, and the ability to shoot-to-kill. Civil liberties groups argue that a human must always authorize the machines' capabilities. But police forces want to activate automatic features in certain situations.*

Civilian drones, unmanned aerial vehicles used in non-combat situations, are everywhere. The machines are used to deliver packages, assist emergency rescue, handle manual labor, and gather close up and detailed information for weather, news and the paparazzi. The acceptance of drones as operational tools in many professions is extended to the use of the machines in civilian law enforcement.

For law enforcement, the capabilities are a mirror of the military's use in war. Police officers can use the drones to chase criminals, disarm them, and even shoot them if the situation arises. Prior to several court cases, every police force developed their own rules on the drones' deployment. And despite an acceptable safety record, stricter protocols were implemented.

For example, drones can be flown in any public space provided the machines are trackable, noiseless, broadcast a unique light signature, and are equipped with sensors to detect humans, birds, buildings, trees and other objects. Drones can be any shape or size. For civilian uses, most resemble the purpose such as boxes for deliveries, but law enforcement uses mini-helicopter style vehicles that can curve around corners like an accordion bus.

Police can use drones as extensions of the human force, "flying officers," anywhere a human officer would normally, and legally, go, a drone can go too. However, once the drone expects to engage with a suspect, it must come under manual human control. For example, if the suspect is wearing a mask, the human operator must have authorization to remotely remove it. If the suspect is brandishing a weapon, the human operator must survey the entire area to ensure the safety of civilians prior to attempting disarmament. And the human officer can activate the drone's weapons only after assessing the situation as if the officer were there live. The operator who fires a weaponized drone is considered to have discharged a service weapon and would be subject to the standard review process.

THE PROBABILITY: Likely that law enforcement drones are already in widespread use but few know where, how or how many.

*

CONSUMER CREDIT

Money Never Ends: Continued access to credit through online protocols

THE ISSUE: *Bankruptcy and credit access issues disappear when consumers default all financial accounts and credit data to automatically search for, and access, any available commercial source of money, including new loans, whenever funds are about to run low.*

Money is whatever we want it to be. If the public believes in the power of the dollar, then it is accepted as a tradable instrument. In a completely online world, physical money, paper and coins are rarely seen, and almost never used in transactions. Instead consumers use cards, or more likely numbers representing cards, for purchases, and allow online applications to automatically pay their bills from savings accounts. When the savings account runs dry, sophisticated applications could automatically search the entire Internet for a new source of funds, scanning thousands of offers from financial institutions to extend a line of credit or loan.

The consumer's pre-defined prerequisites from a cap on the amount borrowed or annual interest rate, to even the location of the funding institution, would define the parameters for an acceptable lender. The consumer's account would then receive approval, before the next bill is due, and the system, without input from the consumer, would transfer the funds, and spending could continue with impunity.

Qualifying criteria applies, and interest rates are based on familiar factors, but the bottom-line is that everyone continues to have access to credit. Performing a function now dominated by high-interest payday loan companies, this service would allow consumers the best rate available anywhere, not just in their neighborhood. The image of families being forced out of their homes by foreclosure fades as online applications crunch available data on employment history, family profile, and reliability to find a solution that prevents the bank from registering a missed payment. This is a scenario where borderline credit consumers would have to provide details for the analysis of their personal online profiles, and allow that information to be regularly updated based on their utilization of the credit services. But, the service provides stability for individuals who would no longer face the fear of losing it all, or of the money ever running out.

THE PROBABILITY: At some point America's debt dependence will run aground and this process will either be a disaster, or used to force everyone back into financial discipline by completing preventing spending when funds are no longer available from weary international lenders.

End of Documents

###

Dear Friends,
I hope you enjoyed The Origin Point. Please post a review of the book on your favorite ebookstore website. Your opinion is truly valuable to other readers and to authors like me. Reviews help other readers find new books and help authors reach their audience. Amazon.com and other ebook retailers consider reviews an example of the author's value to their website and provide additional promotional options to authors with a lot of reviews.

For more information about the Life Online world and all the links to my books, please visit my website http://www.claneworld.com. Thanks for being a reader.

Hope you stay on the side of the thinkers, all the best,

Case

Want to keep discussing future tech issues? Do you have a Book Club? You can download a FREE PDF copy of Dallas Winter's excerpted summary of the 2100 policy files from The Origin Point at Case Lane's Spinning World http://www.claneworld.com/life-online/the-mystery-files/

Did you just finish reading The Origin Point? The novella ended at the beginning of the Life

Online Files book series. What happened next to Louis Santino and the controlled world of the next century? Read the bonus excerpt Chapter One of The Motion Clue to find out.

About Case Lane

Case Lane is a global writer, traveler and observer to the future. Educated in communications, political science, business, law and economics, she has lived and worked all over the world as a reporter, diplomat and digital media corporate executive. Building from her interests in international relations and technology, Case envisions a next century world where the essential battle is between the advancement of technology and the instincts of our basic humanity.

The Life Online book series mixes globe trotting technothriller suspense with the social policy conflicts quickly arriving with the new tech age. Place yourself among the characters who like the majority of people are non-technologists who have to learn to live and manage in a digitally-controlled world they do not understand.

Connect with Case Lane

At my website http://www.claneworld.com

LikeFollowShare

Twitter @CaseLaneWorld
Facebook Case Lane World
Goodreads Case Lane's Author Page
Google+ Case Lane World

THE LIFE ONLINE BOOK SERIES

YOUR FREE COPY IS WAITING

From the author of the Life Online Book series, **The Power of Preparation: 10 Things to Do Before the Future Arrives** is a free guide to help you learn about the steps to take today to be ready for tomorrow.

Click here to get your free copy
OR
Go to Case Lane's website and click Send My Free Copy

BONUS READING

Here is Chapter One of The Motion Clue: A Future Tech Cyber Thriller, Book One of the Life Online series. Each Life Online book can be read independently. Enjoy...

Chapter One of THE MOTION CLUE: A Future Tech Cyber Thriller by Case Lane

Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding.

Justice Louis Brandeis, United States Supreme Court, dissenting in Olmstead v. United States, 277 U.S. 438 (1928)

CHAPTER ONE - THE BROKEN SILENCE

An intense burst of energy surged through a plain plastic and copper data cord. Internally, the physical piece of hardware succumbed to the overload pressure created by an unexpected wave of digital code. Externally, the cord burned until the wire split in half, and the pieces fell into the organized rows of connectors hanging, u-shaped like jump rope, between the server racks. No human saw the break happen, and no human intervened. On monitor screens from twenty feet to eight thousand miles away, an error message appeared. Error messages occurred from time to time, then disappeared after a Network fix. By design, The Network functioned on a continuous, seamless, unyielding schedule programmed to direct all electronically-managed activity. But to The Network's surprise, this error message was not reacting to the design.

Louis Santino, a burly, 43 year old former professional football player from down south in Fargo, North Dakota, was the technician in charge, the only human located at the 148-acre hydroelectric power facility on the craggy lakeside in northern Manitoba. Inside the fiberglass walls of the main Control Room, Santino could not see the error message displayed on a monitor two feet above his line-of-sight. He was lying across his chair watching a football game. Enraptured by the competition, Santino kept his eyes on the screen, his ears tuned to the loud volume, and his body balanced across the industrial furniture. Like many humans, he relished viewing a spectacle of men engaged in dangerous, physical hand-to-hand competition. To keep the game at levels of continuous brutal contact, professional football players wore body armor shields. Fans logged on to watch hulking men of swift athletic skill tangle with skilled players with lightening hands, directed by coaches using thought strategies to outwit their opponents. Eagerly anticipating trick plays, spectators waited for the novelty of witnessing humans execute unpredictable options by using only their brains and bodily strength. But the coaches also used The Network. They had computer applications, called apps for short, running pattern simulations on completed games, and analyzing player moves and statistics over his lifetime. Still, most fans ignored the programmed assistance in favor of the thrilling live play.

Santino focused on the intensifying game action until, without warning, the words 'Alert Signal' displaying in 64-point red block letters, flashed, like the bullet from a firing gun, directly in front of his eyes. Shocked into a swiftness that recalled his own playing days, Santino jumped straight up and out of his chair. Having never previously seen the alert message projection function used, he stood stock still in the center of the room. Without prompting, the game volume on the viewing monitor decreased, and The Network switched his viewing preference from 'live' to 'record.' The Network knew Santino would continue watching the game at a later time, and its automatic behavior prediction feature reacted by saving the broadcast for him.

As his shaking legs settled into an upright place, Santino slowly lifted his handheld com to eye level. All of the facility's operations, the signals, reports and alert data, could be tracked through his com, a palm-sized, flat-screen, black-rimmed, plastic electronic device he had strapped to his belt. All communication devices, or electronic tools with similar features, were called a com even though the equipment had a range of fading names like phone, radio,

television, camera, personal electronic device, or palm, because most literally fit into a hand. Some were branded after fruits including berry, apple, cherry or orange, but those were favored by children. The choice of size, shape and materiel used to manufacture coms was almost limitless, but all had one shared function, all were wirelessly connected to The Network.

People in cities usually kept the com functionality attached to a part of the body like the wrist, or to clothing like a flap on a shirt pocket, but Santino preferred holding the physical device, and the feel of identifiable material between his fingers. The display screen fit snuggly into his large hand tightly grasping the edges as he guardedly read the message The Network was displaying - Employee Intervention Required - for an error, an electrical shortage on the grid in Sector 2G. In sixteen years on the job, Santino had never received an alert requiring him to personally engage in an error repair action. Puzzled, he took a deep breath and began to feel slightly anxious.

Within the minute passing by, a transport silently rolled into the Control Room, and the sight of the driverless vehicle prompted Santino to jump again. The transport, an IO Rider for indoor-outdoor, was sized and shaped like an old snowmobile, with a closed, clear fiberglass box cab on top, and space for two passengers sitting one behind the other. With functionality to hover forward, backward and sideways, or move on bare floors, carpet, gravel, grass, cement, ice, snow and heated terrain, the Rider automatically adjusted to the ground beneath its wheels. Santino stared at the transport and his anxiety deepened.

The Network had processed Santino's transport preference against the intended destination, detected his com location, cross-referenced his image from the surveillance camera in the Control Room, and sent the Rider directly to where he stood. Knowing Santino had little history of leisure walking, certainly not to the distance of Sector 2G, and almost never in winter temperatures, The Network calculated he would not walk to the error location. With his profile, even if Santino had preferred to walk, the transport would follow him, and his com screen would not change instructions until he accepted the ride. He had no override code for the transport's operations. Without another option, he climbed into the Rider, and as The Network registered the pressure of his buttocks on the seat, the cab door slowly closed. Santino did not want, or have to, look at the dashboard screen in front of him as the data updated to display the destination. Although all of his next required actions were automatically uploaded to his com, he was too confused to view the information.

The Rider departed the Control Room, but as the vehicle approached the facility's garage style exit doors, the wheels rolled to a stop at a walk-in closet lining one of the walls, and waited next to a table holding a set of clothing neatly separated from other varying sizes hanging inside. Using Santino's already stored measurements, The Network had selected a coat, snow pants, hat, scarf, gloves and boots, and arranged the items, distributed by conveyor belt, at the closet entrance. Santino stepped out of the transport and walked up to the table. He did not examine the clothing, which was not only his size, but also his color. Putting the items on, he would not normally question why he was dressing warmly, but a flash in his memory considered that if the transport had stopped for winter clothing, The Network not only wanted him to go outside of the facility, but also to step out of the vehicle. The building temperature was a comfortable 71 degrees Fahrenheit, and Santino was wearing jeans and a t-shirt. Outdoors the atmosphere was minus 20, but now in January, the biting air would feel like minus 36. The vast, empty expanse of semi-permafrost and razor thin trees encircling the complex was an occupied home dominated by black bears and gray wolves. The facility at Grand Rapids, the westernmost outpost of Canada's Hudson Bay Hydroelectric and Water Reservoir Complex, was on the 53rd latitudinal

parallel, north. In winter, the terrain was surrounded by ice and snow as far as the eyes could see, and there was no cover from the elements. Humans rarely ventured into the open air as part of their daily functioning. The outdoors was for adventurers, sportspeople, environmentalists, and the occasional daring family with children who wanted to ensure the next generation knew about natural trees and flowers. In cities, both icy and tropical weather populated areas had connected most buildings through tunnels, underground shopping centers, transport stations, subways, overhead crosswalks, and covered people movers. Designated industry employees, like agricultural managers, occasionally worked outside, but only when The Network signaled a problem that could not be remotely fixed, which did not happen often.

Fully dressed for the temperature change, Santino returned to the Rider and, still avoiding the dashboard panel, stepped in and sat down. A few extra seconds would pass as the Rider recalibrated his weight to detect he had sufficient cover for his required pending activity. Satisfied, the transport closed its door and moved towards the garage opening. On approach, the garage door began to rise, and at exactly the spot where the entry panel was three feet over Santino's head, the transport crossed from the controlled environment of the facility into the unmanaged wilderness. The moment the transport cleared the exit, the door rolled back down. The silent descent was not unknown to Santino, but he turned back to follow its close. From his vantage point, the entryway was a gray cut in a wall of snow, unknown as the access to a billion dollar facility currently without a single human inside the walls. As the transport moved forward, he continued to watch the door shrink and fade away from sight.

Despite being inside a heated cab, Santino immediately felt the bitter cold. Living in the North did not inure him to experiencing the region's winter. As the Rider followed an expected path to Sector 2G, the wind whipped around the transport, and cut through gaps in Santino's additional clothing. Defrosters kept the cab windows from fogging and icing over, and he could see the mix of nature and human destruction all around him. The facility's land was covered in short pine trees, limping in the frozen bog of winter, black and white in every direction. But the man-made structures were gray and silver, cement and steel walls pushed up against a body of water, flowing even in the cold, as liquid rushing through the barrier with a force turning the world's largest turbines, and pushing electrons out over wires for thousands of miles. Santino did admire the engineering, and all of the details required to create the facility, but the construction operated on a relatively ancient design, vulnerable to terrorists, remote and disruptive to the natural environment. Clean air had a price, humans had learned that lesson decades ago.

The Rider traveled 50 mph, and for a minute Santino considered he had no idea where Sector 2G was located. When he had first obtained the hydro job, he had been told not to expect to know the layout of the complex, The Network would lead him to any location he was required to visit. But in his idleness with the employment's tasks, he would scroll through distraction options on his com, which led occasionally to searching The Network to view maps and blueprints for the facility. Coms had an endless array of features, but the only portal for accessing all functions was The Network. Every business used The Network for operations, administration, sales tracking, inventory ordering, marketing and forecasting, and since employees needed the information for their work, instant access was available through their coms. The same device facilitated personal lives by displaying The Network links to data inputted into computers as text and voice communications, government records, education results, employment opportunities, sports scores, movie reviews, consultations, nutrition advice, weather warnings, and all other information stored on globally-connected servers. Recorded movements from cameras and sensors tracking the timing and changes in human activity were

automatically stored on servers too. The Network continuously scanned servers, even those not exposed to the public Internet to retrieve, cross-reference, and integrate data within controlled spaces. Aggregated data was used to create and send appropriate daily life instructions, specifically prepared for each individual's com, and all other coms interacting with an individual. Avoiding The Network was considered impossible. Some people tried diminishing its role in their lives, but few completely avoided the functions. The Network managed personal lives, businesses, organizations, and government operations with efficiency and accuracy, directing individuals throughout the day, and even allotting time for relaxation and socializing. Millions of programs and apps recalculated and redefined data every second, and the data fed the human's com, and the human reacted accordingly.

But The Network did not ignore the surfing of its own files. If an unexpected search pattern was recorded, a protocol determined if the issue should be escalated. After Santino had executed several similar search requests about the facility, The Network had sent a text message asking him to define the information he was looking for, and the reasons for his search. After one warning, if an employee persisted with unexplained research, The Network would implement a punishment tailored to the employee's preferences. When Santino had tested the protocol once too often, The Network blocked his access to Internet sports and entertainment sites for 24 hours. He had been left with the silence of the Control Room. Since that day, he had not bothered to look at the facility's layout again.

Without an awareness of his current location or intended destination, Santino patiently sat as the Rider continued to fly across the terrain, automatically making speed adjustments to account for the surroundings, the activity in the area, and the presence, or lack of, other vehicles. All transports had sensors for assessing the environment around a route. If no other movement was detected along the travel path, the transport could accelerate across the snow and ice like the wolves in pursuit of prey in the forest nearby. Santino let the wind, snow and trees pass by him as a cascade of debris from a sneeze, and considered for a moment that he might be enjoying the ride. But when the vehicle began slowing down, his anxiety returned. Sector 2G arose no special memories for Santino. He was not near the main dam, but out along the high voltage electrical power lines running away from Grand Rapids to all defined destinations. The dashboard was displaying the coordinates for the area, but he was still not interested in registering detailed information. As the Rider came to a stop at the base of an electrical transmission tower, Santino leaned back against the seat, and the cab door slowly opened.

Looking out into the bleak of the fading daylight, Santino waited for his instruction. But after another minute, he realized the transport would not be in talk mode. He was one of the few employees who hated voice instructions. Transport voices could be any modulation, a soprano lady, a child, your own, but Santino preferred not to respond to electronically-spoken instructions. Other people did not mind, especially if they were around humans all day. But Santino had decided in the absence of working with humans, having a computer talk to him seemed a little desperate. His home system had available voice commands, but since The Network already knew he had most audio turned off, the system waited for him to read his instructions from the Rider dashboard screen or his com. Choosing to ignore both options, Santino braced for the cold and stepped out of the cab. A sensation overcame him he rarely felt, surprise. He stared up at the rising extended stretch of tower steel, glanced down at his com, and back at the Rider.

The transmission tower was one of thousands of identical steel structures built to the sky on needle-like precision that minimized wind shear and maximized height. Santino could not see

the top, only sensor lights illuminating in red, yellow or green, offering the same advisory as streetlights. At first glance, all he saw was green. But as he looked straight up the spine of the tower, another shockwave slowly rolled over him. Santino felt the unfamiliar sensation again, surprise, cloaked in an even more unexpected awareness of rising trepidation. In the near night sky glowed the unmistakable purple light of a hovering drone.

Unmanned aerial devices operating one hundred percent automatically on instructions from The Network, or automatically with a human override, or one hundred percent by a human with a manual remote control were, by common understanding, a drone. The machines could be any size, and had a variety of functional uses including carrying products from instruction documents to packages to emergency kits to repair tools, to assisting with construction and structural repairs or disaster rescue, and targeted surveillance. Drones could be any geometric shape even balls or triangles, or resemble miniature versions of helicopters and other flying machines. For delivering packages in a city, drones were predominately one-foot square boxes, but for military maneuvers in the desert, the machines were the size of single-passenger airplanes. Humans co-opted the name 'drone' from military aircraft used for missions in the last century's desert wars. The military and drone manufacturers had desperately tried to encourage an independent civilian name for the machines, but the term had long ago passed into popular use, easy to say, spell and remember. With unlimited specs, drones could also be manufactured in a variety of facilities, and be equipped with weapons, legally or not. Businesses, organizations, professionals and individuals ubiquitously used civilian drones in all aspects of their daily lives and operations. Humans appreciated the conveniences provided by the machines, and most were placidly comfortable with the devices moving above them at work, in streets, parks, homes and office buildings. Drones and humans were considered completely compatible.

On an industrial site, the machines were work-tools, programmed to lift heavy objects, patrol remote facilities, and ferry goods around complexes. By law, the devices emanated a unique fluorescent light created under patent through a color simulation of royal purple and aquamarine blue unavailable for use by any other aerial object. Civilian drones had to be distinguishable from every other status light or active device in the sky. All recognized nations had signed a treaty solidifying, for governments, companies, and international service organizations, the unified rules for the use of commercial drones. In most countries, individuals could own personal drones and the action lights could take on any hue. But the status light color humans and The Network saw, as the drone moved through the sky, or hovered nearby, had to be drone purple.

Santino recognized the purple light, but not the drone. His apprehension rising again, he looked at his com to search for the drone's identification record. But there was no report and no displayed coordinates for a drone in the vicinity. He hit 'Refresh,' and the screen re-emerged in less than a second. His instructions were still there, but no drone indicator. Confused, Santino knew he should not be able to see a drone's light, if there was no drone. Repair drones were stored at locations all around the complex, and The Network could dispatch one to any location to fix an operational problem. But the system would never send a human and a drone to look at the same error at the same time. If animals or the weather had damaged a line, drones equipped with cameras, mechanical arms or industrial equipment, could make the repairs without humans. A human employee could view the repair operation from the Control Room using the fixed surveillance cameras, the repair drone's camera, or even dispatch a specific camera drone to record the action. Company management or law enforcement could also dispatch camera drones at any time to look at incidents around the site. The Network would recognize the internal

instruction and update an employee's com. Occasionally a specific authorization was required to be advised if a drone was on site, but that advisory usually depended on security issues, which Grand Rapids never had.

Santino's puzzlement was quickly turning to outright fear. He desperately considered if the situation had a valid explanation. He wondered if he was looking at a camera drone a human monitor had sent to view the error. Although he was the only human at the complex, he was not exactly alone. The electronic surveillance was extensive and omnipresent. The complex's operations could be monitored from the company's operational facilities 1,100 miles to the south in Kansas City in the United States. After Kansas City, the data was continuously backed up to a server farm in Iceland, and its backup was in Liberia. Because hydroelectric power was a strategic and vital resource for millions of people, the Canadian Defense Force Command Centre near Ottawa monitored all of the connected sites, and the North American Defense Command outside Denver monitored all monitoring. Mexican officials kept their eyes on activity from their surveillance complex in Toluca, west of Mexico City. The Chinese and Europeans were also likely to be paying attention, but their surveillance was not considered official, and was politely ignored. At least one Santino-level employee, but not many more, worked at every monitoring site. The locations were responsible for continuously viewing all security at all energy plants, reservoirs, sub-stations, and along thousands of miles of transmission lines stretching across the North American continent. Santino expected the individual who sent the drone to be aware a human was at the same location, but it was also possible human operators did not have the same information. Disturbingly, he had no definitive idea which options were operational. He had never interacted with the information, equipment and protocols available to the monitoring teams around the world. He could only be almost certain, although not completely, that The Network would detect any drone at the complex, and he should be able to see the detection on his com. 'This is strange,' he considered, looking around. Grand Rapids had 10,124 cameras and sensors, all visibly on. Each networked security device could register the difference between a black bear, wind, an authorized human employee, and an unauthorized intruder. An unknown, unidentified detection would trigger an intruder protocol. After analyzing evidence from camera and sensor data, The Network would activate an investigatory drone to deploy to the incident site. Since the company had the right to be advised of all drones inside its complex, if this one was not an authorized drone, the unauthorized intrusion protocol should already be in progress. Either way The Network must be aware a drone was here and inform the human employee. Santino should have the information on his com, but he did not.

Abruptly, the sound of metal cracking ice emerged from the Rider. Santino spun around to face the sight of a ladder unfolding from the transport's side panel, and ascending like a stretching coil up the narrow steel edge of the tower. The transport remained parked alongside the base, and Santino observed the action with increasing nervousness. The ladder inched up, and at every two-foot mark automatically unrolled a clamp to attach to the tower's frame. Although The Network could continuously measure the voltage traveling in any direction, and the chance of a miscalculation was negligible, the absorption ladder was a precaution used as a barrier to protect humans from electrical currents. If charges were unbalanced, The Network sensed and corrected the difference, by redirecting electricity across the appropriate wires to cut voltage to an overcharging section, or increasing production to one reporting a shortage. Santino eyed the ladder's resolute rise up and out of his sight. Holding his com up to eye level, he noted his next displayed instruction was to climb. He moved over to the affixed steps, but stopped and stood with one foot on the lowest rung. Sucking in a deep breath of the ice-laced air, he

uncomfortably realized he had come all of the way out to Sector 2G, and did not know why. 'What was the repair work that could not be completed by a drone or The Network?' Feeling increasingly unnerved in the bitter Canadian cold, Santino finally decided he should read the entire Network error report.

Gripping his com, he scrolled the text back to the point where the error message had first appeared. All company messages were configured to a specific employee by prior education, experience and duties. If an engineer pulled up the same report, the details would contain technical language and schematics, for Santino the display was basic points explained in plain English. The report began with the surcharge, but did not state the source, next were instructions he had already witnessed, leading to the pending step for a human action to ascend the ladder. None of this information was a revelation to Santino, but the fact he was standing out in the cold did not add up. Now if he wanted to return indoors, he would have to follow The Network instructions or the transport would not process his efforts and take him back inside. The temperature felt like it was dropping by the minute, forcing his questions and concerns to be clipped at the same precipitous pace.

As sheer spots of frost began to develop on the waiting ladder, Santino realized the error must be unrecognizable by a drone or The Network, or both, and this possibility terrified him. He was a technician, not an engineer or an electrical tower designer. 'What did The Network conclude he could do?' The report on his com had stopped at action for a human, and he was the one who had been brought to the site to complete the task. 'Maybe this was some new, unknown type of damage.' Although The Network could assess any error, and determine a repair protocol, an unforeseen problem may have intervened with the process. Suddenly, Santino felt better. 'Yes,' he decided. 'It's an unknown type of damage The Network cannot interpret, that's why a human is required.' But as he began to climb the ladder steps, apprehension swept over him again. 'What could be an issue he would encounter that The Network could not detect, analyze and manage on its own?' All information was in The Network, all of the data humans knew. The entire hydro complex - the electrical systems, transmission towers and programming for the servers - had been designed and built by computers. As Santino climbed the ladder, he ached to imagine the problem he would find, and failed to process any potential scene.

Rising up the transmission tower were sensors placed at two-foot intervals. The tower stood at 216 feet, and his com indicated a red light flashing at marker 56, 112 feet up, high enough that as Santino began to climb, he would not be able to see the sensor above him until he drew nearer. As he continued to ascend, another confusion wave rolled over him. Part of The Network's standard error assessment was to send photos or video of the problem for review prior to transporting the employee to the site. Yet he was climbing without any diagnostic or repair tools. After only visually noting the error, he would have to input findings into his com, and wait for The Network to determine his next action, including if necessary, delivering required tools. With each step Santino's incomprehension soared. The lack of visuals, he realized, must be an error within the error.

A minute later, reaching the 100-foot mark, he emerged into the unidentified drone's defined purple glow illuminating the flat black sky around him. By silently hovering, the drone complied with laws protecting birds and other flying creatures from audio disruption to their natural rhythms by man-made airborne devices. But the accommodation ended there. The machine was a two-foot square box coated black except for one side featuring a clear plastic viewing window, a popular feature Santino enjoyed because a human could see directly in to the electronics. Despite the ease with which drones fit into human life, an interior view reminded

humans, the drones were machines. Unlike flying creatures, drones did not require wings, but many people, the opposite of the interior-view types, added the feature as if to reassure themselves the machines were more ecological, members of the bird family, and not an output from a gadget factory. The movement of the box reflected its gravity-defying support. The device made an almost imperceptible rocking motion, adjusting up and down and side-to-side, which aided in remaining steady in the blowing air. Seeing the drone waiting with balanced calm, Santino stared and offered, under his breath, a slight moaning "hmm" as a greeting when his eyes and hands reached level with marker 56, 112 feet above the ground on the transmission tower in Sector 2G.

"Good evening," the machine greeted him in a clear, steady news announcer's voice.

The drone's verbal reaction locked Santino into a reflexive shock. His hair stood up at the back of his neck, and his hands gripped the ladder frame as he thwarted an instinct to jump. Drones did not talk. Not only could a human turn off all talk instructions from Network-connected electronics, but also by law and common practice, company drones, law enforcement, military, all standard, work-related drones, did not talk. Emergency rescue drones had a speaker function humans used for communicating in disaster areas when drones were used to look for survivors. And many civilians had personal talking drones. But flying a talking drone in public airspace with the talk function turned on was illegal. Under no normal circumstances would a drone dispatched to an industrial work site talk, no circumstances at all. Drones were not robots, robots could talk, and everyone knew that. But governments, and most citizens, did not want to hear talking from boxes or bags with wings. Public spaces were already disturbed by the miniaturization of coms, making humans always appear to be talking to themselves. But the confusion would escalate if tens of thousands of inanimate objects also spoke randomly and simultaneously aloud. Part of the ease felt with the flying devices humans had come to tolerate was awareness that the machines did not talk. "A talking drone," Santino whispered under his breath, while glancing at the box. The machine did not reply. Santino could now hear his own heart beating loud and fast beneath the layers of winter clothing. 'A talking drone,' he silently repeated, staring at the machine. For the first time in the evening, he was absolutely certain the incident was not routine, but forced outside of his experience, education, training and knowledge of human life. Drones did not talk. Humans and drones were not sent to repair the same error at the same time. And the error at marker 56 was not an error that had ever been seen before.

*

Khadrian Laltanca could not believe she and Roman Francon had managed to be in the same place, at the same time, for more than one night, for the first time in two months. She stared at his naked back as he lay face down beside her in bed. Over his torso, she could see the peaks of the Rocky Mountains in Colorado breaking through the horizon as snow sprinkled the frozen ground, and crystal snowflakes formed on the window. 'The best way to enjoy winter is indoors,' she thought slipping deeper beneath the down blanket, and closer to Roman's warm body.

Their relationship had begun exactly where prohibited, at a top secret international conference where they were not only representing different countries, but were also on opposite sides of the issue. Every time she had made a point in counterclaim to his delegation's argument, he would look at her from across the meeting table and grin. If his action had been a negotiating tactic designed to attract her attention, he had been right on track.

At the time, she was one of her country's top strategists, working behind the scenes to allow private companies to build technology infrastructure projects in other countries, without revealing the nation's research and development secrets. A diplomat and a lawyer, Kadie

interacted with every interest group, balancing their demands against one another in search of a viable solution. Within the past year, the United Nations had asked her to take on the same role for the world, Commander of the U.N. Security Council Special Command for Cyber Security, the unit within the global security organization authorized to address and settle cross-border cyber conflicts. The U.N. role was her official post. But an obscure global group called The Alliance had solidified her professional future by reaching out, quietly as they always did, to place her among those who showed notable promise as unfaultable global leaders. Working outside official channels, The Alliance preferred to encourage people who had multiple ties to countries around the world, transitional language skills, and the ability to blend in among individuals as diverse as a medic in a refugee camp, or a donor at a ten-star charity dinner. The unseen organization was even more specifically impressed that she had independently built her skills, a natural was always an unfailing bet over the groomed. The naturals knew the life they wanted and pursued their objectives without regard to obstacles falling onto their paths. The groomed always needed a little handholding. Kadie had grown up on the flat dry lands of the upper Midwest, and worked her way through increasing levels of education, with one clear objective in mind, independence. She preferred to be her own boss, but if she had to answer to a higher ranked official, then that person had to be a broader thinker than she was, an individual from whom she could still learn. Kadie traded jobs when people failed to live up to her expectations, resigning was her way of not settling, of always extending to achieve more than the envisaged.

Roman knew the profile, and had noticed her attributes the moment he had seen her at the conference. Having studied the biographies of the participants, he had memorized her picture and resume. And once he saw her at work, he finalized his assessment. Kadie was intelligent, attentive, precise, fair, and fun, in his analysis, a female version of Roman Francon. But she was a natural, making her singularly more attractive on every level.

In contrast, Roman was the definition of the groomed, he had been born into The Alliance. His British father, Landon Francon founded one of the largest financial investment firms in the world, Francon Global, and he was The Alliance before the group was invented. Although the organization did not encourage nepotism, members did take recommendations from their own, and when Roman independently showed his promise, he was accepted into the organization soon after earning a commission with British Intelligence. Landon had married a Colombian hedge fund owner, Camilia Fernandez, who was richer than he was. They raised Roman and his five siblings, all over the world. But New York City was usually home, and the entrenched preparatory schools lining the U.S. Northeast coast were the setting for their education, at least part of the year. The rest of the time, they were learning in Europe or China or Colombia, living in the cultures and languages their parents determined were important for their future. The Francons did not shy away from relentless ambition. Landon and Camilia had no intention of allowing their offspring to fall into the middle class, or even upper middle class. They insisted the children fill their brains with knowledge, even while owning the technology allowing them to bypass memorization. They had to learn to construct with their hands, fluently translate, and solve mathematical equations without a computer. Roman had hated his parents' insistence on human brain-captured data and information, until he began to understand the life they were trying to maintain, and the separation that had come upon the world between those who paid attention, and those who did not.

In the five-star suite at the Silver Deer Lodge in Aspen the flames from the fireplace were down, but the room remained at a comfortable room temperature, 'probably too warm for

Roman,' Kadie thought, pulling the blankets down to their waists. She was naked too, lying face up. As she rolled over on her side to run her fingers through Roman's hair, she caught a glimpse of his com, flashing. Grinning, she whispered, "Nice boy, you turned off the sound." But her contentment quickly faded, the com was persistently flashing, firing in red, and she of all people knew exactly the implications of the color of danger. Carefully she reached over him to pick-up the com from his side of the bed. Looking at the screen, she turned towards him with shrinking joy, and crawled on top of his body. She placed the com at his closed eyes, kissed his lips, and whispered into his ear, "Somebody wants you."

*

"Sunlight," Santino spoke aloud, holding his voice steady, trying not to tremble in response to the persistent cold nor the waiting drone. He carefully watched as the drone slowly turned over its light, the purple beam faded to the back of the box and a glowing yellow-white light emerged in front. Like transports with headlights, drones were typically built with illumination capabilities from the straight-line beam of a flashlight, to the unraveled cone shaped rays mimicking a child's drawing of the sun. Around Santino, the intense darkness was sliced off at the edges, brightening marker 56, the tower, the ladder, his clothes, the trees, and even the stars shining in the night sky above. Santino adjusted his eyes, blinking repeatedly. Slowly the brightness broke his fear, and made him feel as if the sense of abnormality of the last hour had only been a flare of ignorance. Drones, he knew, responded to specific voice commands. But when he dared to look back over his shoulder, he saw darkness again, and stillness. The simulated sunlight he was receiving was only the limited offering the box was programmed to deliver. Restricted to the instructions on his com, Santino had no choice but to accept the words and carry on. Instinctively, he held his com to the light even though the added brightness to read the screen was unnecessary. The device continued to display an error message for marker 56, but provided no further pinpoint location accuracy. As steadily as his senses stabilized, Santino felt nervous feelings returning. If the drone had been dispatched to check the error, a pointed light should have been directly aimed at the reported problem, instead the machine hovered, waiting. Santino held his com up over the marker, and selected the 'Locate' icon for the error. The device narrowed its light, Santino stared in the direction of the beam, looking up and down and around, but the entire frame appeared exactly as he had already observed.

"This is ridiculous," he declared, abruptly pulling back his com and shutting off its light. No updated instructions appeared on the screen, and no further report was generated. "Okay..." he continued aloud, "...this is the error." The idea made him shudder, but he could not imagine another explanation. No visible problem could be seen, and neither the drone nor the com was pointing to an exact location he should review. Even the tower's status lights, illuminating only in green, confirmed his assessment. Santino looked in all directions for red or yellow warnings, but none were visible. Sinking further into distress, he considered that if his suspicions were correct, he had another problem. 'How could he tell The Network, the error message was wrong?' The Network had sent for human intervention and was stuck on an instruction. Without a human taking action to repair the reported error, The Network would not react. If Santino tried to leave Sector 2G without fixing the error, he would need manual control of the Rider. But with no override code for the transport, if he wanted to return to the Control Room, he would be forced to claim an emergency.

On the average workday at an industrial site, there was no human emergency that could not first be analyzed by The Network. The Network had to view or detect incidents, and review the data to determine whether to authorize an override code. Emergencies had to be specific, a

human had to be in physical danger or be suffering from a sudden ailment requiring human intervention. But at this point in the 22nd century, most diseases were rapidly eradicated. When unknown illness symptoms manifested, blood samples could be extracted at an automated biolab, located in shopping malls, large office buildings, on university campuses, at residential high-rises, or even the hydro complex, and sent for analysis to World Health Organization certified labs. Data about every reported ailment was being collected and processed every second, and global health labs produced antidotes, vaccines or other cures based on collated information from around the world. A broken bone would not help either. A com could detect the status of bones in the body, and an onsite medical drone could perform a laser-soldering stabilization procedure before ambulance transport arrived at the facility. Failed internal organs were typically the only option left for obtaining immediate medical contact with another human, but he would actually need an organ to fail, the diagnosis had to come first from The Network.

An employee at the largest hydroelectric complex in the middle of North America could not use the excuse of a medical emergency to obtain an override code for transport to take him back inside, because he was cold and confused, and unable to find an error The Network had been reporting for over an hour. Other types of emergencies would have to be verified with video from a camera feed or sensor data on The Network. If he tried external help, no employee at any monitoring station would understand a disruption instigated by a human, and not The Network.

Desperately he tried to imagine other statements he could make or ask The Network that would trigger an override or response to, at least, allow him to go back to the Control Room. If The Network had detected an unfixable error, and the detection was actually also an error, maybe reporting, 'no visible issue,' would prompt The Network to recognize a human action, and change its instruction. Deciding the possibility was worth a try, Santino held up his screen and entered the code for a human action resolution. The detail screen appeared and he stared at the features. Using a drop-down selection for previously used standard reasons for required human intervention actions, he searched for the simplest option, 'Unable to fix.' Although he doubted his attempt would be successful, he added 'no specific location for error indicated, no problem visible,' in the comments box, and touched, 'Submit.' The screen read 'Resetting,' but a second later the message returned to, 'Error - Employee Intervention Required.' Sadly, Santino conceded his idea, as he suspected, had not worked. He wondered if a human monitor on the other end would see his message, maybe he should have entered more information. Quivering in the brisk air, he contemplated his options again. If he contacted a monitoring station, he assumed the other end could view only the same instructions, and probably tell him he had to find the error. He thought about walking back to the facility, but he was on the opposite side of the complex, maybe ten miles or more from a human entry point. Humans could only use their com, face or hand scan to enter doors on the south or west side of the building, he was to the northeast with only transmission towers around him. He would not be able to use the Rider entrance on that side either, because the garage doors were only programmed to open for transports with entry instructions.

Santino struggled in the sinking cold, 'what to do?' he wondered. He kept looking at the com hoping the screen would suddenly display another instruction. He hit the manual 'Refresh' icon again to see if the information would change, but it was the same. After another minute, he began to speculate about touching the wire and casings at marker 56, to determine if there was an issue he could feel, even if he could not see an obvious problem. Or he could simulate a fix to trigger a Network reaction. In his subconscious, he knew the idea was ridiculous. The Network was precise. If he reached out to shake the wire, sensors would register the movement had taken

place at the touch of human fingers or a tool. But the system would not register a fix unless the error was genuinely fixed. Still he was out of ideas and getting colder. If his approach did not work, he would brace for questions he could not answer and contact a monitoring station. He turned back to marker 56, looked again at the area where the error had been detected, and shined the com light back over the spot. Since all of the wires were high voltage, he would not directly touch a line. Instead, he would shake the edges of the frame connected to the wire. Although the action seemed trivial, sometimes there really was only a hair out of place. Slowly removing the glove from his right hand, he decided to use his bare fingers to initiate The Network's cross-reference of his fingerprints with the authorization records. If an unauthorized person touched the equipment with bare hands, sensors would trigger an alarm and the pre-determined security response, dispatching camera drones to the site. But his prints should only create an authorized notation.

As Santino's skin came into contact with the frame in front of him, a whirring sound of a slowly revving jet engine rose from the drone. His hand stuck to the tower, Santino froze again. Civilian drones operated silently, gliding through the air without engine or machine noise. 'But this sound…' he questioned, '…first talking and now…noise? Who operated civilian drones that made noise?'

*

"Yeah she's a hot chick and she's been fooling around with me all night," Roman light-heartedly moaned into his pillow. His eyes were still closed as he spoke, and Kadie pressed her weight against his back.

"Sorry my love," she said with melancholy. "Open your eyes."

Roman opened his eyes prepared to roll her underneath him, but the first visual he saw was the glowing red screen of his own com. "What?" he proclaimed taking the device from her hand, and holding it at eye level. Kadie rolled off and lay beside him.

"It has probably been flashing for a couple of minutes."

"Yep," Roman responded, entering text into the device. He rolled over onto his back, hand on his forehead to hold back his hair as he read. After a minute, he stopped and looked at his girlfriend.

"Problem?" Kadie asked, knowing that was all a flashing red message could be.

He leaned over to her face, the com and his hand brushing against her breasts. "Sorry my love," he entreated, kissing her. "Good morning." He moved to sit up with his hand still holding the com, and continued to text. When he finished, he stood up. "Electricity has gone out."

"What?" Kadie instinctively looked out the window where streetlights twinkled in the darkened Aspen streets.

Roman followed her gaze. "Not here. From Canada, moving down the center grid towards Kansas City."

"What's moving?"

"I do not know, my love," Roman replied, as he walked towards the bathroom.

"But what are you talking about?" Kadie theoretically knew electricity could go out, since there was always a miniscule but possible chance of simultaneous catastrophic failure in all active and back-up distribution locations at the same time. But redundancies in the inter-locking grid maximized resources. No blackout of any length had disrupted a developed country for decades.

"I'm talking about an electricity shortage," he shouted back to her over the sound of running water. "They are re-routing from James Bay, but people are without electricity."

Kadie could not believe the news she was hearing. "But why are they contacting you?" she shouted back. Several minutes passed before he reappeared, wrapped in a towel, water droplets dripping off his skin. "Why are they contacting you?" she repeated.

"Security issues, baby," he replied, slightly exasperated as he began to dress.

Kadie rolled her eyes at him. She had a higher security clearance level than he did. "I know it's security," she retorted. "But what?"

"I don't know, but I've got to go." Roman had swiftly shaved, groomed, dressed, and holstered his gun. She always marveled at how rapidly he could prepare for the day. Catching her anxiously watching him, his demeanor shifted. Walking towards her, he leaned down to kiss her lips, before politely adding, "I'm unbelievably sorry, but I have to leave you to go and deal with an international emergency." He stared into her softening eyes. "I love you, and I'll let you know the moment I know what is going on."

"Security permitting," she warned as she kissed him back.

"Yes of course, security permitting."

"I love you too. Be safe."

He smiled, kissed her again and turned to leave. As the door closed behind him, Kadie picked up her com and began looking at overnight messages. Neither Kadie nor Roman were officially in Aspen, and they certainly were not known to be sleeping together. Kadie had no reason to know there was an emergency on the North American electricity grid. But she looked for a search route to the details of Roman's alert notification message that would not be uncovered by The Network.

As government monitoring of free public Internet activity had grown increasingly intrusive, technologists from around the world, highly skilled engineers and computer programmers declaring no affiliation to a government or business or non-governmental organization, had built a separate internet. Initially, they had only known how to hide their server farm physical infrastructure, but not digital signal transmission equipment permitting instant global access. The situation dramatically changed when the acceleration of personal travel to outer space, expanded into personal cargo shipping, and people with resources launched their own satellites faster than any government could legislate against the practice. Since shooting down satellites could lead to war, the private civilian launches created a crisis. Almost all commercial satellites had been controlled by public companies, not wealthy individuals operating behind shell corporations. Governments tried to outlaw private, individual satellites, but lost all of the court battles. The technology was too advanced to claim interference with national security, and the territory of the earth's orbit was too substantial to demand more than limited control over its expanse. If individuals adhered to the operational treaty agreements of their home governments, the satellites were legal.

Although governments could use their own satellites to monitor all others in the sky, on the ground the rogue techs, as the independent technologists came to be known, had sliced the electromagnetic spectrum to carve out private lanes in the virtual cloud to untraceably carry their data. They called these electronic roads off the public information superhighway, off-ramps. The governments knew the off-ramps existed, but whenever their official technologists reached an identified entry point, they could not find a way in. Rogue techs had built impenetrable firewalls, coded multi-level encryption keys, created redundancies around the world, and most importantly, attracted the support of billionaires who had wanted a secret, but accessible internet for their personal use. The work was a volatile risk that changed every day. Rogues, with deep-pocketed friends, managed to build and re-build their off-ramps and private networks, faster than

governments and law enforcement could find and infiltrate them. The rogues considered the challenge of creating virtual construction projects the greatest videogame ever played, and a battle they had to win. When they had uncovered the most efficient means for traveling back and forth between their servers and the worldwide Internet, while virtually masking the access to their off-ramps, the separate, secret networks proliferated. Although conspiracy theorists warned that people were delusional if they thought governments did not have control over every bit of data, those who could afford rogue tech assistance bought access to an off-ramp, and the software to use their coms while masking the activity from The Network. The switching was seamless from a Networked com, Global Intelligence rarely knew who was on private off-ramps around the world. And although technically, government officials were not permitted to access the unofficial entry points using their high security level coms, unlike most people who were monitored for the activity by The Network, presiding officials like Kadie, were not.

She projected a screen in front of her eyes, and using an off-ramp, accessed a private global news forum for government and industry officials who cared about sharing non-public information. The site had been built and populated through virtual word of mouth, as a portal for invited members to anonymously post information they could use in negotiations and international discussions. The contributors saw the confidential bulletins as efficient diplomacy, their governments would likely have another word for the practice, disloyalty. But claiming disloyalty was an overreaction, a threat to limit the actions of thinking people. True disloyalty put millions of lives in danger, their knowledge sharing, saved millions.

Kadie navigated to a forum site. Users entered information in their own languages and had developed their own coded terms. If a user were serious about staying up-to-date, she would have to master the ability to read other people's coded comments. Quickly Kadie wrote, 'Driving into dark near Kansas today, looking for divergences on the road?' Expecting the wait for a reply would not be long, she hit 'post.'

*

Louis Santino and the box drone were at a standstill. The whirring sound had been brief. From the moment Santino had expressed alarm and stopped moving, the noise had halted. Staring at the drone, the human literally felt the drone staring back. The air around him had ceased to be cold, instead Santino felt the heat permeating from his body as he sweated from head to toe. His fingers were gripped to the tower frame, not attached by frostbite, but by his own terror of not knowing if movement would trigger a drone action he was not prepared to manage. As he considered the position of his hand, the simulated sunlight he had nonchalantly requested minutes before, began to fade.

"No, no, don't!" Santino proclaimed aloud as the sky encircling him transformed from the comforting soft white glow to the background of a seamless black night. If a human had sensitive eyes, The Network would have the drone slowly adjust the light. But Santino did not have sensitive eyes, this drone should have instantly switched the light off only on his command. With growing awareness, Santino determined he would not be providing any more instructions to a box acting on its own. He desperately wanted to look at his com, to see if updated information had appeared, but the slowly setting simulated sun told him an action would probably come too late for official or unofficial word to reach him. As the light faded completely out, a red laser beam flashed on and aimed its pointer directly at the spot where Santino's hand grasped the frame at marker 56.

"No, no, *Santa Maria*, no!" Santino shouted. He had seen the work of red laser beams on news programs. "No, no, no, off, off!" he cried as the drone once more increased the volume of

its whirring sound. "No, please no!" Santino begged the box. With his screams reverberating in the empty dark forest where bears, wolves and deer had long ago been frightened away, and chased deep into the trees by the construction of the hydroelectricity complex, Santino expected no response. Launching reflexive actions to prevent capitulation to the waiting darkness, he moved to lift his hand off the frame, and direct his feet down the ladder. But the drone stopped prepping. Before the human could make his retreat, the machine revved up the force and intensity of the beam, and the whirring sound mimicked the extraction of a firing mechanism. The red laser reconfigured as a singular heat source directing its trajectory towards Santino's hand, through to a green-lit sensor on the tower, and at impact, set off an explosion bringing down the transmission tower in Sector 2G.

Alert signals lit up monitoring stations all over the world.

*

When Roman arrived onsite in response to the earlier text alert, more than one person in the meeting room was completely startled to see him. He was equally disconcerted. For the past several weeks, he had been working inside a military complex in the mountains between Aspen and Denver, Colorado, with an officially non-existent Western Hemisphere Defense Command strategy team. A digital security mask overrode the global position indicator on his com, and broadcast his location as Dallas, Texas, his status read 'On Business.' The gathered attendees he now viewed, representatives of eleven countries and organizations, were not the same people he had been seeing every day at WestCom to negotiate a revised security agreement for Central American countries. Instead, this group was military and industrial officials, contacted by various organizations to assemble and hear specific information.

In a room containing a long oblong table, short at one end, wider at the other, and built on a slight rise, every person could clearly view the rest of the seated attendees. At each chair, translation sensors were embedded into the armrests. An individual's com would detect the spoken language and, if necessary, feed a simultaneous translation into an earpiece. On one wall 90-inch video conferencing screens were positioned to project as if the displayed individuals, who were in other locations, were sitting in the room. Another wall broadcast news and satellite images. The last supported a refreshments table with the preferred beverages and snacks of every participant ordered and available based on a Network predicted calculation of the amount each person would consume, within the scheduled time they would be meeting. Roman was hungry, but he would not have time to reach the food table.

"What's going on?" were the first words Roman heard upon entering.

"I'm sorry General, I received the same message you did," he politely replied to U.S. Army General Patrick Wheeler. "I have no other intel." Wheeler inattentively looked at him, and Roman quickly moved to take his place among the representatives.

On a video screen, Slater James, an agent at British Intelligence in London began speaking, "We have been monitoring a situation at the Grand Rapids hydro dam in Canada."

"What kind of situation?" Roman asked.

"The incident was a glitch," answered the hydro company's representative Corey Miller, a senior executive with military clearance for the meeting. "A fried or split line led to an outage. But we cannot get a complete report."

"You do not know the problem?" questioned Eduardo Juarez, the ranking Mexican military officer based at WestCom.

"It's a big facility, could be any issue. But the real problem is, we have no credible Network report," Miller glumly stated. The complete hydroelectric complex provided zero carbon

emission, always on electricity, to the populated areas of central North America, north to the mining and military towns in the Arctic, and south down the Pan American highway from Winnipeg to Minneapolis to Kansas City to Dallas to Monterrey and to Mexico City on through Tegucigalpa to San Jose and ending a few miles south of Panama City. Each of those centers transmitted electricity in a hundred directions to the skyscrapers of the big cities, factories in commercial zones, acres of agricultural production sites, and small forgotten towns along the routes. The towering transmission lines rolled out from sites like Grand Rapids at high voltage across empty plains, and upon reaching populated areas, the lines went underground, or where necessary, disappeared to continue transmitting virtually, through the air. Most humans had never seen a power line. As a stable, reliable energy source managed through a treaty, almost all military installations within range also connected to the complex. Despite its limited use of human employees on the ground, Grand Rapids was a vital location affecting millions who obtained at least part of their living from its existence. The center of North America was the crucial infrastructure reinforcement for the mega-populations and ports on the coasts. The strategic inhabited centers in the Pacific Northwest, around the Great Lakes, New York City, in Northern and Southern California, Texas, South Florida and Mexico City contained nearly three-quarters of the continent's people. Those regions had self-contained networks, energy, and water supplies, but almost all back-ups were in the center, on the Hudson Bay grid.

Miller continued, "We have a lot of data being analyzed, cross-ref—" He halted as an alert signal sounded, and the room fell completely silent.

"Please look at the monitors everyone," Slater directed. "We have now been advised the incident was extended."

The video screens switched to scenes of the disaster at Grand Rapids, smoke drifted over a crumpled heap of steel where the transmission tower in Sector 2G had once stood. The entire room gasped. At the destroyed site, a dozen wheelbarrow-sized drones acted as water cannons, and dosed the embers from the explosion fire, while a camera drone, programmed to detect body parts, scanned for Santino. Human investigators had been dispatched to the scene, but all of the initial information to be analyzed was already captured in The Network. The meeting room participants rapidly activated personal screens from their coms and simultaneously read The Network's report.

"This is your glitch?" shouted Wheeler. "What is this?"

"No, no, this happened..." Miller frantically clarified, reading the report on his com, "...this happened after. The security camera pictures show a drone—"

"But this is unbelievable! There is no drone on this report, only the man."

"What brought down the tower?" Roman asked.

"The situation was all routine," responded Jayna Luongo, another security cleared corporate executive. "An error was detected and an employee was sent to look."

"But why a human? The report does not say what went wrong." Roman was also quickly looking at the details on the report.

"There was an error."

"But what does that mean? There's no diagnostic for the error."

"Did the employee make a mistake?" Miller asked.

"Doesn't say," Luongo replied. "There was an error, an employee was sent to look, and a drone—"

"What drone?" Roman asked.

"Whose drone?" Wheeler demanded. "Report does not say that either."

"The Network recorded the transmission tower had an error, but there is no confirmation as to what or why," Luongo continued. "We only have surveillance pictures of a drone...umm...attack. That's all we know. But those pictures cannot give us any more details."

"But what kind of drone was it?" Wheeler asked again. "Was there military activity in the area?" Military and law enforcement drones could be weaponized with the ability to deliver a range of disabling impacts from the effects of stun guns to missiles. But operating a legal, weaponized drone required adherence to laws, regulations and protocols, sanctioned and used almost exclusively by governments. If the rules had been followed, a few of the people in the room would have the details available on their coms, but they did not.

The questions flew across the table as Roman stood up, and walked up to a 50-inch screen displaying a live camera feed of the smoldering scene at Grand Rapids. 'What an extraordinary explosion,' he thought. 'Enough to bring down the tower, an entire transmission tower, but how?' He looked closely at the images. The tower had collapsed straight down, straining adjacent transmission lines, but not creating a domino effect. The wire casings were set to automatically snap, and avoid pulling another tower down if one fell. In fact, the attack, as the incident was now being referred to, seemed to have been neatly organized only to collapse the one tower with poor Louis Santino. 'But was Santino necessary?' Roman wondered. 'Why didn't the attacker isolate the tower? Why kill one human too? What was this? What kind of terrorist organization or anarchist was after them now?'

"Listen everyone, please listen!" Slater shouted to restore calm. "We have been watching this site since the outage was first reported. Consider this next information confidential and the reason we called you here. This information has not been widely disseminated but...the attack drone...this is the third incident worldwide that we know. But this is the first one to knock out power. Whoever this is, he is getting bolder. And whatever technology they have, we cannot identify the capabilities. Every time an incident has occurred, we have had to find the drone visually, using satellite pictures, there was no detection on The Network."

"What do you mean no detection?" Wheeler asked. "Network cameras and sensors are always checking the entire space around—"

"No, excuse me but we do not have continuous checking, as you say," Slater corrected him. "If the intruder drone is emitting an electronic signal, The Network would detect the disturbance through the complex's sensors. For most security protocols, if the detected signal is within camera range, we'll immediately get a picture or video record. The system analyzes the picture and identifies the object in the captured image. The protocol only looks for detected signals. Only objects with a detectable signal can be detected unless the known object has a previously identified distinct sound like a buzzing bee, or a particular feel, like the touch of a human hand. If no object is detected, the picture will not be analyzed, a human would have to launch a manual request, if the human even knew to look for the problem in the first place. Whatever that box is, it has no detectable signal."

"But that's impossible!" Luongo cried. "How can a drone fly around without a signal? A human must be in control."

"Maybe this is an advancement in drone operation, Ms. Luongo," Slater countered, slightly annoyed. "Some of our enemies have technology we do not have."

"Or we do not officially have," Roman said.

The room fell silent. "And the destruction? We have not heard about that before, what a mess," Wheeler added. "Humans will have to clean up."

"Drones can do the heavy lifting," Miller assured the group.

"Not before we've examined every inch of the place."

"I am afraid we are only likely to find dead wolves," Slater ruefully commented. "We will not find evidence of any use to us."

Roman tried to concentrate. 'We won't find any evidence,' he thought. 'We have to catch him, whoever he is. We have to figure out the pattern, what he's doing and why.' He looked around the room. 'We'll never move forward with these people.' Holding his com under the table to avoid appearing distracted, Roman sent a text message to Slater.

"Listen up!" Wheeler shouted over the clamor. "Our analysts will look for clues in the data, but in the meantime, what do we think is going on here? Terrorists? Industrial sabotage? Who?" The room went silent.

"We have had three attacks, three completely different locations," Slater added. "There's been a solar farm in Botswana, a wind farm in the North Sea, and now hydro power in Canada. The only connection among the sites is renewable energy. But for the first two, the facilities did not really lose power...or a life."

"And this time, kaboom." The General dramatically flung his arms into the air.

"Yes this saboteur has escalated the attacks."

The people in the room looked at each other. They were political appointees, friends of leaders, and business people with money, in general, not the people with the experience and patience to strategically think through the incident, and make implementable decisions. Roman moved towards General Wheeler.

"We should ask for an emergency U.N. Security Council meeting," Wheeler commented. The clamor of simultaneous shouting began again.

"And tell them what?" Juarez demanded.

"To be careful, to change security protocols."

"But for what? What explanation can we give?"

As Roman approached, he spoke clearly and directly, "General, we do not need a U.N. meeting. We immediately need to bring in the right people to get to work on this. This is an ongoing international problem, not one incident. We need a team that can think this through, figure out what's going on and take action."

The General stared at him. "Of course people," he said pointing to the room as if to indicate he knew what people were, and he had them right in front of him. "What are you talking about?"

"With all due respect General, not people who talk," Roman continued. "People who think. People who would have a better understanding of the issues we could be dealing with."

"People who think?"

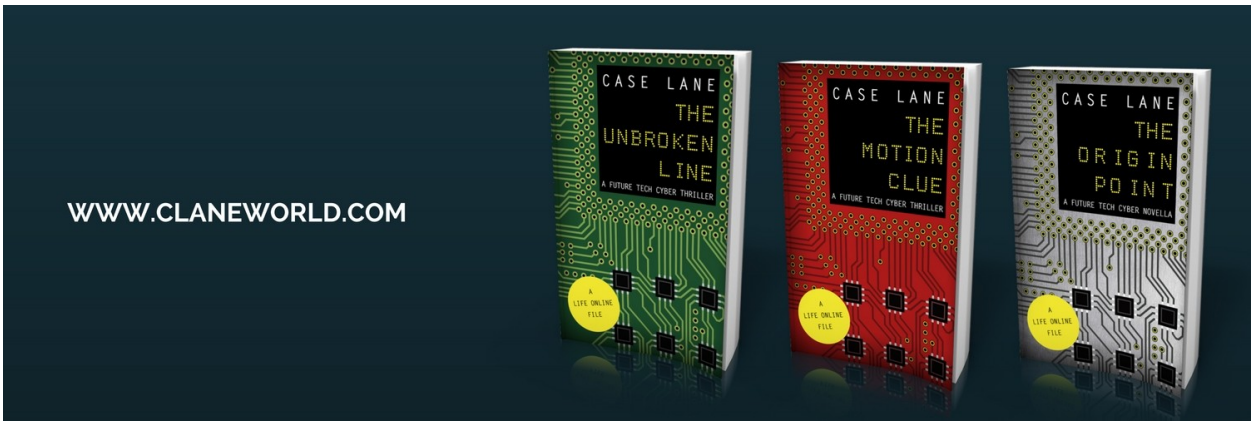
"I agree, General," Slater interjected. "A different type of group is required to manage these incidents."

"Whoever did this has access to some amazing technology," Roman stated. "We need people who have experience in these areas. We also need to be ahead of this perpetrator, to be on top of his potential next target. We need to identify the right people, get them collaborating, and let them figure this out."

"The right people?" Wheeler asked puzzled. "What people? Who?"

"I know who," Roman confidently replied.

*



You can find The Motion Clue and all Case Lane books at your favorite e-bookstore website.

For more information visit Case's website http://www.claneworld.com

Thanks for reading,
Case Lane

*

[Back to the Top](#)