Prologue

Burkett
July 9, 2021

In the four years since appearing on the Internet, the individual known as Factor Man has reached out to exactly five human beings. In spite of this minimal contact, he (or she) is now one of the best known, richest and most powerful men (or women) on the planet.

Of those lucky five, all but one are now ridiculously famous. There is the New York lawyer, Robert Hasday. Concierge services for Factor Man are provided by the social organizer Jess MacMurray, known to the world as Pepper Potts. No one knows the name of the member of the hacking group Anonymous who has worked with Factor Man, but everyone knows what that hacker did. And there is the reporter William Burkett, who has very mixed feelings about all of it.

The fifth person is not so famous. He's a banker named Brian Finn. The fifty-something retired ex-president of Credit Suisse. Balding. Overweight in spite of his best efforts not to be. An extremely good guy, as far as I can tell.

Finn and I met over coffee about six months ago. I have no idea if I was followed or not. Sometimes I'm followed, sometimes I'm not followed. I don't really care either way any more.

Finn gave me an envelope, and then we talked about Finn's role in the leveraged buyout of RJR Nabisco in the 1980's. I wrote a story comparing the buyout frenzy of the 1980's to the Internet bubble of today, and no one seemed to realize that my meeting with Finn wasn't about the 1980's at all.

It was all about the envelope. Inside was the story of Finn's interaction with Factor Man. Brian told me it was okay to write about it, provided that no one learned of his involvement until the day before FCOP. Factor Man's instructions, he said. I agreed to not even look at it until a week before FCOP.

Finn isn't Factor Man. He doesn't have the background. I don't think Finn even knows who Factor Man is. He might, though.

But it doesn't matter. Tomorrow, we'll all know. FCOP. Pronounced Eff-COP. The Factor Man Coming Out Party. And Brian Finn is going to be one rich son of a bitch.

My name is William Burkett, and I'm the reporter. People claiming to be my friends call me Wilbur. Orville would be worse, I suppose.

This is the story of the last four years. And if we hadn't all lived through it together, no one would believe a word of it.

1

Factor Man
May 12, 2017

Werner Heisenberg was a physicist born just as the nineteenth century ushered in the twentieth. He made such significant contributions to physics that he won the 1932 Nobel Prize for creating the field of quantum mechanics. He had an uncertainty principle named after him. He figured out how stars worked.

This last contribution has always struck a personal chord with me. Rumor has it that some time shortly after Heisenberg figured this out, a friend commented to him one evening how beautiful the stars were. "They are," Heisenberg is said to have replied. "And I'm the only person in the world who knows why they look that way."

I stared at my computer screen. This was my Heisenberg moment, I figured.

My computer had two windows open. In one, numbers streamed by slowly. In the other, an email waited to be sent. Twenty-one words that might change the world. All I had to do was click on send.

But once those twenty-one words were out there, I could never get them back. So before clicking send, I thought about it.

I thought about the science.

I thought about Denise, down at the barn working with the horses. Even after many years of marriage, they would always be her first love. If the email changed my life, it would change hers with it.

I thought about our kids, no longer living at home and beginning to make their own way in the world. If I sent the message, they would be making their ways in a different world than they had explored yesterday.

I thought about my plan. I wondered if my family and I would be safe. I wondered if I would indeed manage to deflect at least the worst of the disruption to which my technology might lead.

And I thought about Heisenberg. About knowing something that only you know, and that you know will change the world in ways you cannot predict. It took a generation for quantum mechanics to beget nuclear weapons, and longer still for the science to lead to a new and clean – albeit dangerous – energy source. My discovery, I suspected, would have as great and as unpredictable an impact, but far more quickly.

I thought about science, and the ethics of science. We scientists just do what we do, and somehow trust that the things we discover will be used more for good than otherwise. It's never been clear that such optimism is justified, and no one ever gave us the moral authority to unleash our personal progress on the rest of the world. But we're scientists. We do what we do.

I thought about Denise, and the kids, and the unknown consequences.

I thought about the plan.

I thought about Heisenberg.

I thought about science.

I hit send.

Burkett
May 12, 2017

I was relaxing, smoking a cigarette, and feeling pretty good about myself. Yeah, yeah, I know. Smoking is bad for you. Hopefully, I'll manage to quit before it kills me.

On this particular night, though, I wasn't worrying about it. An article I had written a few months previously with a statistical analysis of Donald Trump's tweets had gotten a ridiculous amount of traction. I'd heard that afternoon that it had been selected as a finalist for an annual prize regarding Best Use of Data in a Breaking News Story.

This is the kind of thing I do. From late 2016 until now, I've been a reporter for the *New York Times*. I owe my job to Nate Silver, who runs a website

called fivethirtyeight.com. 538 presents news (and sometimes predictions) based on statistics. Nate started his life as a quantitative analyst doing sports statistics, and applied the same techniques to predict who would prevail in various political contests. For example, he called every state correctly in Barack Obama's presidential victories in 2008 and 2012. He's basically gotten everything right since then, too, except for the Donald Trump thing. No one saw that coming, although Nate was closer than most.

Anyway, Nate got famous and the website, which was owned by the *New York Times* during the 2012 election cycle, was responsible for something like a sixth of *all* the nytimes.com traffic. When Nate switched to ESPN before the 2016 election, the *Times* decided they needed to replace him with a statistics group of their own. They hired a bunch of young hotshots, and I was one of them.

On that night in May of 2017, I was twenty-eight years old, with a new Ph.D. in statistical economics from the University of Texas at Austin. I loved my job, which was to use statistics to figure out cool stuff. Predict who was going to win the world chess championship. (Yes, humans still played chess.) Analyze the words in Donald Trump's tweets and show that they bore more resemblance to the rhetoric of the alt-right than to any form of rational discourse. The *Times* gave me a great deal of slack on the writing side, allowing me to duplicate the informal style that Nate used at 538.com. Unusual for a major news outlet, but totally fine with me.

I lived in Brooklyn, in a two-bedroom apartment that's a third floor walkup. I don't have to tell you this; I still live there and you've seen the apartment on TV and the Internet. Reporting may be the best job in the world, but the pay is only modest. Maybe I'll try to negotiate a better deal for myself after FCOP – the Factor Man Coming Out Party – is over. Until then, though, I've got enough to worry about.

Nowadays, I miss my privacy. Smoking that cigarette and relaxing on a Friday night in May four years ago, I didn't even have a Wikipedia page. I was just getting started at the *Times*. A bunch of folks in ridiculously small circles knew who I was, and that was about it.

That was all just fine with me. As a kid, my heroes had been Batman and Robin, folks cool enough to appear in comic books and with attitude to boot. By 2017, I looked up to Carl Bernstein and Bob Woodward, the reporters who broke the Watergate story. Reporting can be quite a noble enterprise,

and my interest in the truth dwarfed my interest in fame or fortune. It wasn't even clear to me that I had any real interest in fame or fortune.

I remember it was raining. An early summer thunderstorm in New York City, around midnight. I stubbed out my cigarette and went to check my email. Six messages.

```
From: tdalton@nytimes.com       you didn't win but great job
From: KBURKETTJR@aol.com        Mom had a great time
From: factorman0@gmail.com      returned favor
From: trindell@wisconsin.edu    rerunning those numbers
From: kate@bedandbreakfast.com best deals of the year
From: emmabhardaway@gmail.com   can't make it - sorry!
```

You see it right away, of course. But all I saw was that it was Friday night, and Emma had just blown me off for Saturday. Well, sometimes life is like that.

So I went to bed.

* * *

Saturday mornings, I play basketball. I pretty much suck, but so do all the other guys. We meet at eight because that's when we can get the gym, play until around ten, and then have coffee.

Eight o'clock is pretty early, but coffee can go on for hours. I tell you all of this only so that you understand why it was a little after one on Saturday afternoon when I got back to my email.

Factor Man would eventually reach out to five of us, of whom four would become known to the public. Finn was the lucky one. The Favored Four, they call the rest of us, although it's not clear to me how favorable it is to live under this ridiculous microscope. For better or worse, I was the favored first.

```
From: factorman0@gmail.com
To: wburkett@nytimes.com
Subject: returned favor

Mr. Burkett:

You did me a kindness once, and I'm returning it.

factorman0.blogspot.com
```

The story is yours, and yours alone, for forty-eight hours.

FM

I checked the time at which the message had been sent. Fourteen of those hours were already gone.

Next, I did what you would have done. In fact, I did what pretty much everyone has already done. I visited the Factor Man web site.

I have a fast method for factoring large numbers. This is a problem, because it breaks public key encryption. And if I figured it out, so will someone else eventually. It's not really viable to simply keep it secret.

To make matters worse, or perhaps better, the method works by converting number factoring problems to Boolean satisfiability and then invoking what appears to be a polytime SAT solver on them.

At some level, this is good. A polytime SAT solver is, in the long term, only promise. We will cure more diseases, and be healthier. We will be more efficient, and better able to get resources to those of us who need them the most. We will be more able to cope with a huge range of problems, not the least of which is global warming.

In the short term, however, a polytime SAT solver is only peril. There will be no more unbreakable codes. And in a world that has become increasingly dependent on them, that means there will be no more secrets.

My hope in this blog is to deal with this issue, to help us collectively achieve the promise while avoiding at least some of the peril. To that end, I will be embarking on a program that involves two separate phases.

The first is demonstration. I need to show the world that I can indeed do what I say I can do.

The second is distribution. I need to make the technology available to everyone.

For the first phase, I will simply factor large numbers in public. The way this works is as follows. If you want a number factored, send that number in an email to factorman0@gmail.com. I will select five

numbers each day and respond in this blog (factorman0.blogspot.com) with the factorizations.

But there are some rules.

1. The numbers must be of a size I specify. Currently the numbers must all be at most 5 bits in size. Hardly a challenge! But every three days, I will permit the numbers to be one bit larger.

2. When you request that a number be factored, you must include legitimate identifying information for yourself. Only one number per person per day, please.

3. All of the numbers to be factored must be the product of two primes.

My hope here is that as time passes, recognizable public figures will ask for ever larger numbers to be factored, allowing folks to understand that I can indeed do what I say I can do.

I will be factoring 64-bit numbers on November 11, 2017.

I will be factoring 128-bit numbers on May 22, 2018.

I will be factoring 255-bit numbers on June 10, 2019.

By 2019, I expect that anyone relying on public key encryption will have found another way to protect their data. I encourage people relying on public key encryption to switch to at least a 256-bit encoding scheme as rapidly as possible. I will not factor 256-bit numbers in public.

After the demonstration phase is complete, I will move forward with distribution. This will work as follows:

On June 10, 2019, I will begin accepting bids for a license to use the technology. The license will be perpetual and will be exclusive for one year. Bids will not be accepted from entities whose goals conflict with the goals of the government or citizens of the United States of America.

On July 10, 2019, I will provide the technology to the highest bidder and announce that bidder's identity.

On July 10, 2020, I will provide the technology to the government of the United States.

On July 10, 2021, I will make the technology publicly available and will reveal my identity as well.

It is my intention to deal relatively harshly with any attempts to interfere with this overall plan by, for example, attempting to bring down this blog or my email address, or attempting to discover my identity before I choose to reveal it. I remind anyone considering doing these things that no corner of the Internet is beyond my reach.

If you would like a 5-bit number factored, please send me an email with both the number in question and your true identity.

And until July 10, 2021, I will simply paraphrase the immortal Tony Stark: I am Factor Man.

The now-famous counter was at the bottom, showing the number of visits the page had received. That counter, as is well known, now shows something in excess of 350 *billion* visits to the Factor Man web page. When I looked at it that morning, it said, "1".

Back then, of course, I didn't really know what most of that stuff meant. But I had a friend who did.

* * *

Every year in March, I go to the American Crossword Puzzle Tournament, or the ACPT as the participants call it.

This may strike you as a fate worse than death. But it isn't. Believe it or not, it's fun.

The tournament is run by Will Shortz, the crossword editor for the *Times*. Held in Stamford, Connecticut, it's attended by about six hundred of the best crossword solvers in America. The 2005 tournament was the subject of a documentary called *Wordplay*.

The event is fun in a couple of ways. First, it's exciting. After solving seven puzzles shared by all six hundred contestants, the top three finishers get up on stage and solve one last, brutal puzzle while everyone else watches. Whoever finishes that puzzle first wins, assuming they don't make a mistake. The finalists (wearing headphones and with their backs to the audience so that they can't hear the raucous commentary going on behind them) announce that they're finished by raising their hands.

In 2015 Dan Feyer, who had won the previous five contests, finished first. But rather than raise his hand, he decided to check his work. The next contestant to his right, Tyler Hinman, had won for the five years before Feyer

started winning. In the five years Feyer had won, Hinman had generally been second.

Hinman was working frantically to finish. Knowing that Feyer was fast, Hinman had decided to raise his hand the moment his puzzle was done.

Feyer was checking. Hinman was writing. Feyer's puzzle was perfect, but he didn't know it. Hinman's was also perfect thus far.

Finally, one of them raised his hand.

Hinman's hand went up half a second later, and the audience exploded. Feyer's streak continued, although it would be broken by Howard Barkin the next year.

The real reason I look forward to the ACPT, though, is the people. Part of what I cover for the *Times* is high-level mental sporting events. The world's best chess players, or bridge players, or what have you, are generally not a lot of fun to be around. Their self-images are too wrapped up in the games at which they excel.

But crossword solvers are somehow different. They all have day jobs. (The ACPT grand prize is only $5000, so they have to.) Feyer is a musician; Hinman is a computer programmer. The contestants include lawyers, authors, reporters like me, and Hollywood directors like Patrick Creadon, who directed *Wordplay*. It's an amazingly eclectic group.

And everyone is there to have fun. With the self-images mostly out of it, everyone wants everyone else to do well. Everyone wants everyone else to improve on their scores from the previous year. The only perennial villain is "Dr.Fill", a crossword-solving computer program. Dr.Fill solves the puzzles in the back of the ballroom where the contest is held. When each puzzle is done, Shortz announces how Dr.Fill did on it; the worse the program did, the louder the applause.

I met Emma Hardaway at the 2017 tournament. I was a reporter, and she was a manuscript screener for a literary agency in New York City. Just a couple of word nerds at the same event. We introduced ourselves to each other while kibitzing a *Trivial Pursuit* game during the wine and cheese party that takes place the night before the tournament begins.

Emma was effervescent and charming. Tall, attractive, well-spoken and smart, but with a wicked glint in her eye that warned against taking her for granted. One of those interactions where you wish afterward you'd exchanged contact information. Well, there was always the next year's tournament.

In reality, though, I didn't need to wait that long. I bumped into Emma in a little coffee shop in SoHo, one of those impossible New York coincidences that make life in the city worth living. This time, I got an email address and – I thought – a tentative agreement to meet for dinner a few weeks later. But my email had said it was not to be.

* * *

A couple of years before I met Emma at the 2017 ACPT, I met Montgomery Grimes at the 2015 event. He wrote the software that handles the scoring for the event, although the puzzles themselves are graded by human judges. (Those judges collectively examine about a million filled-in squares over the course of the weekend.) More interestingly, Grimes is the author of the villainous Dr.Fill, which he steadfastly refers to as "it" instead of "he". Dr.Fill finished 55th in 2015. Grimes gave an entertaining talk about how the program worked, and I included it in the article I wrote for the *Times* about the event itself.

When not working on Dr.Fill, Grimes is in steadfast denial of the fact that he's in his early sixties. In addition to running three startups (Mark Cuban is an investor in two of them), he and I have exchanged email over the years about a variety of his – for lack of a better phrase – mad schemes. He thinks he can use a couple of high-definition cameras and computers to figure out which way a rebound is going in basketball – while the shot is still in the air. Grimes believes he can explain birds' flocking as a mechanism to make evolution more efficient. He raised his kids on a diet of stories about a guy named John Gizmo, who bails them out of all manner of trouble with gadgets like the *cat transporter*, which is the size and shape of a flashlight but can hold millions of cats, the *beginning end*, which turns back time in a small area, converting the most hardened criminal into a crying infant, and the *gezuntifier*, which disables anyone who sneezes. I figured Monty was a smart guy and could tell me what was up.

```
From: William Burkett (wburkett@nytimes.com)
To: Montgomery Grimes (montgomerygrimes@gmail.com)
Subject: take a look?

Hey Monty:
```

Can you take a look at factorman0.blogspot.com and tell me what you think?

Thx

William

Grimes is a weird duck. When you send him an email, he generally responds within five minutes. Doesn't matter what time it is. I don't understand how he does it. I wonder if his wife does.

From: Montgomery Grimes (montgomerygrimes@gmail.com)
To: William Burkett (wburkett@nytimes.com)
Re: take a look?

Whoa. This guy is really smart.

Our email dialog continued.

Burkett: You feel like being a bit more specific?
Grimes: Is this real?
Burkett: I was hoping you could tell me. What does it mean?
Grimes: Too much for email. Telephone?
Burkett: Sure. Give me a few; I'll call you.

When Grimes says telephone, he means telephone. Not Skype, not FaceTime. I don't know if this is because he's ridiculously old school, or because he lives out in the sticks and his Internet connection is terrible. Could be either one.

He picked up on the second ring. "Hey."

"So what am I looking at here?" I asked. He explained it to me, or at least attempted to.

"Okay," he began. "Lots of problems involve what computer scientists call 'search'. That's not search like Google; it's search like looking for a needle in a haystack."

I mumbled something generally encouraging, and he continued.

"Imagine you're trying to go to a movie on a Friday night. It's 8:17, the movie starts at 8:35, and you're the kind of person who really hates being late for a movie. Can you get to the theater in eighteen minutes?"

"Sure," I told him. "The movie is only five minutes away from my apartment."

Monty ignored me. "One way to figure it out is to consider every possible path you might take. You head out of your driveway, and can go either right or left. Let's say you go right. Thirty seconds later, you come to the end of your block; now you can go straight, right, or left. You can also turn around, but that's clearly dumb. Let's say you turn right again. After thirty more seconds, you get to another intersection. More choices." Telephone or not, I could see him, walking around and waving his hands as he got into the topic.

"In fact, there are a *lot* of choices. Say you can get to about thirty intersections in the eighteen minutes available, and there are three possibilities at each intersection. So there are three choices at the first intersection, and each of those has three successors at the next intersection. That's nine possibilities. And each of those nine has three successors; you're up to twenty-seven. By the time you deal with all thirty choices, you'll have considered about…" He paused for maybe five seconds while he figured it out. "200 trillion possibilities. By the time you think about them all, the movie will not only have started, it'll be over. It'll be over and so will the sequel – if you consider a million possibilities a second, it would take about seven years to check them all."

I told him that if I was in such a hurry, I would just pull up Google maps and let my phone figure it out. People did, after all, tend to make it to movies on time.

"But even Google maps can't look at 200 trillion possibilities on your behalf. So how do they do it? Is there any way for them to tell, with absolute certainty, that they're giving you the most efficient route?"

"Presumably. That's why they have the app."

"But how does the app *work*?" He paused again, doubtless waiting for me to add an explanation.

I disappointed him.

"Here's the trick," he told me. "Instead of labeling each possible path by the amount of time it takes, you label each *intersection* by the amount of time it takes to get there. You start with the intersections next to your house; they're easy. And since you can always tell how long it takes to get from one intersection to another, you can gradually label intersections further and further out until you know how long it takes to get to the movie theater.

Voilà! Organizing the calculation this way, it takes about 900 steps instead of trillions."

"Okay. I think I'm following. That's how my phone can tell me when I'll arrive."

"Exactly," Monty answered. "But now let's think about a different problem. One summer," he said, "you decide to go on a giant road trip with your family. The plan is to visit every state capital in the continental United States, starting and finishing at your house. But you have to do it in three months, because that's when your kids need to be back in school."

I told Monty I didn't have any kids.

"Pretend," he answered.

I pretended.

"Can't do it," I finally said. "It's a stupid trip and no one in their right mind would spend three months with their kids in the car."

"Suspend your disbelief."

I suspended. I told him I had no idea if it was possible or not.

Grimes paused, no doubt waiting for me to say something more insightful than, "I have no idea." I disappointed him again.

"Fine," he eventually continued. "Let's think about this together. Suppose we decide to start with Albany. We know we can figure out pretty easily how long it will take you to drive to Albany from your house."

"Apartment," I corrected him.

"Whatever. Apartment. And then if Trenton is next, we can figure out how long it will take to drive from Albany to Trenton. So once you decide in what *order* you're going to visit the cities, it's not too hard to figure out if a trip that uses that order can be completed in three months. With me?"

Given our earlier discussion about how long it would take to drive to the movie, this made sense. Yes, I said. I was with him. He continued.

"The problem is that there are a lot of possible orders. In fact, there are over 12 novemdecillion ways to do it, where novemdecillion is a word you don't hear terribly often and probably don't want to. It means 1 followed by sixty zeroes."

"So twelve novemwhatever possibilities are a lot," I told him.

"Novemdecillion. More than a lot. It's too many to consider in any reasonable amount of time," he concluded.

"I can see that," I answered. "But couldn't we just figure out some new clever trick that lets us solve this faster? The family-vacation problem doesn't seem that different from the get-me-to-the-movie-on-time problem."

"They are different," Monty told me. "The trick we used before, labeling intersections instead of paths, doesn't work here. The city orderings seem like the basic things that we're considering."

"Okay," I said, encouraging him to continue.

"It turns out that no one knows if the family vacation problem can be solved in a reasonable amount of time or not," Grimes told me. "It's actually called the 'traveling salesman' problem by computer scientists, since it started by trying to figure out how long a traveling salesman would need to visit all his customers. The movie-on-time problem is called the 'shortest path' problem."

He kept going. "And think about it."

"Stop," I said.

He stopped.

I mean, he just *stopped*. Silence on the other end of the phone line. Finally, he asked, "What?"

I told Monty my brain was full.

"I'm just summing up," he answered. "If you want to know how long it will take to get to the movie, your phone can tell you. But what if you have to run errands, and you have fifteen places to visit before coming home. What order should you run them in? *There's no app for that.* That's the traveling salesman problem. The shortest path problem is somehow easy, and the traveling salesman problem is somehow hard. That's the real reason that Google maps exists but the event sequencing app doesn't."

I was surprised. "So this stuff actually matters in real life."

"It does. And 'easy' here turns out to mean something specific called, 'solvable in polynomial time'."

I interrupted again. "You call this summing up? Use words of one syllable that I've heard before."

Monty paused before continuing. "Fine. This. Guy. Says. He. Can. Solve all things fast. Like the trip thing. As fast as God can solve things."

I couldn't believe he was actually doing it. I told him not to be an asshole.

"This 'Factor Man' can make any problem easy," Monty told me. "Any problem at all. It's as if he can just guess the answer to anything, so that all he

has to do is check that his answer is right. You want to guess the right order to visit the capitals? He can do that."

Grimes paused, and I said nothing while trying to figure out what all this had to do with factoring and prime numbers. "He can solve any problem?" I asked.

"Yes. Any problem. The consequences would be profound, and not just for traveling salesmen. You want to break a secret code? Factor Man can guess the key."

"So there could be an app for that," I answered.

"Exactly. There could be an app that would let you hack into any system, decrypt any secret message. But that's only the beginning. Drug design, for example. That typically involves finding a protein that takes a particular shape. Computing the shape of a specific protein is easy, but guessing what protein to use is hard. Factor Man can guess, and drug design just got easy.

"You can play a perfect game of chess by always guessing the best next move to make.

"Even mathematics is easy. Recognizing a valid proof of some hard result like Fermat's Last Theorem is easy; finding the proof is hard. Factor Man is claiming to be able to just guess the proof and be right every time."

"He could solve anything," I summarized.

"He could solve anything." Monty went on to tell me that the algorithm Factor Man claimed to have, one that would allow him to make omniscient guesses that solved any problem, was called "God's algorithm" by computer scientists. Of course, most people believe that God's algorithm is reserved for God, and that mere mortals can never be so inspired. Grimes quoted MIT's Scott Aaronson, who had said that if God's algorithm existed, then "the world would be a profoundly different place than we usually assume it to be. There would be no special value in 'creative leaps,' no fundamental gap between solving a problem and recognizing the solution once it's found."

But Grimes, the mad scientist, disagreed. His view, he said, was that God's algorithm existed after all.

"Why?" I asked him.

"Because I don't think God would keep the best algorithms to himself."

Geez. Only Grimes would turn code breaking into a question about God's personal attitude toward the rest of us.