Book Review: *Dark Wire: The Incredible True Story of the Largest Sting Operation Ever*, What Happens When the FBI Tries to Monopolize a Market?

Allan Shampine & Nathan Wilson*

Introduction

In *Dark Wire: The Incredible True Story of the Largest Sting Operation Ever,* Joseph Cox details how from 2018 to 2021, the FBI secretly ran a company selling encrypted phones to criminals. This firm was named Anom, and it produced and distributed customized mobile handsets with a specialized operating system and an encrypted communications app also called Anom.[1] The FBI's effort, code named Operation Trojan Shield, provided extensive information on criminal operations around the world.[2] While the story itself is well worth reading from a general interest perspective, this book review appears in an antitrust publication because the FBI's efforts provide fascinating examples of practices and issues familiar to antitrust practitioners. Moreover, they illustrate how businesses and consumers may respond when legal remedies are not available. In this review, Anom's history is explored through the lens of antitrust economics.

One of the goals of Operation Trojan Shield was to move criminals to Anom from other encryption platforms. In economic terms, one could say that the FBI wanted to monopolize a product market for encrypted handsets in geographic markets outside of the US.[3] The book discusses developments in both product and geographic markets, including the challenges of manufacturing and distribution as well as the competition between different products and between distributors of the same (as well as differing) products.

The story of Anom, and the outcome of Operation Trojan Shield, are well worth understanding to appreciate that a black market is still a market. Moreover, behavior in an illicit market can be profitably viewed through the lens of industrial organization economics. It is interesting to see how customers protect themselves when legal protections are unavailable, and how effective, or ineffective, those strategies are in the absence of a legal backstop. Indeed, it is remarkable that in spite of customers lacking any legal protections such as antitrust laws, and in spite of the FBI

■

Allan Shampine *and* ***Nathan Wilson*** *are Executive Vice Presidents at Compass Lexecon.*

**The authors are Executive Vice Presidents at Compass Lexecon. Various claims and allegations discussed here are disputed and litigated. The authors are not involved in those disputes and take no position on the veracity of the claims and allegations. This review is focused only on the economics associated with the story as presented in the published book.*

1 Joseph Cox, Dark Wire: The Incredible True Story of the Largest Sting Operation Ever (2024).

2 *See* Press Release, U.S. Dept. of Justice, FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown (June 8, 2021), *available at* https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive.

3 The legal structure for the operation was complex, but in brief, sales were limited to outside the US, and intelligence was actually gathered by foreign agencies and then passed on to the FBI.

being able to literally shut down large competitors through state action, various market factors appear to have made the FBI's monopolization efforts to secure a large share of sales relatively ineffective.

Background on the "Market" for Encrypted Criminal Communications

In this section we discuss different providers of encrypted communications, differences between them, and patterns of entry and exit. This background is helpful when thinking about how Anom fits into possible product markets.

Criminals have always been interested in secure communications, and enforcers have always been interested in accessing those communications.[4] With the widespread adoption of smartphones in the early 2000s, many criminals began using encrypted messaging services such as BlackBerry Messenger that were provided by consumer-facing enterprises. Some used these services on standard handsets, relying on the app on the handset being encrypted and the app provider being unwilling to work with law enforcement. Others went a step further and used modified handsets that contained additional security measures.

Firms with integrated hardware and software solutions have entered (and exited) the broader encrypted communications space on a regular basis, as have app-only firms. Over the past decade, a number of firms focused on selling dedicated hardware and software solutions to transnational criminal enterprises. Those firms included Phantom Secure, Encrochat, Ennetcom, MPC, beStealth, Ciphr, Sky ECC, No. 1 BC, and Anom, among others.[5] This is the group of competitors that *Dark Wire,* and the FBI and its international counterparts focused on.

In reviewing these products' history, *Dark Wire* tells a story of quick substitution of communication methods in the world of transnational crime. For example, in 2016, Netherlands police announced that they had obtained traffic from the Danish encrypted handset company Ennetcom, which was then shut down. At the time, Ennetcom was reported to have around 19,000 users.[6] One group of criminal users in Scotland then vertically integrated, forming their own company, MPC, which subsequently began offering service to others. The pattern of one encrypted device's death precipitating the growth of others is a theme throughout *Dark Wire*. As of 2018, MPC in its turn was estimated to have around 5,000 users.[7]

Other former Ennetcom customers went to a company called Phantom Secure, which sold modified BlackBerry smartphones that had the camera, microphone and GPS physically removed. Phantom Secure phones' only local functionality was encrypted text messaging. The company also marketed the ability to remotely wipe users' handsets as part of the sales pitch for the product.[8]

The CEO of Phantom Secure was a citizen of Canada, where his company's operations were legal. However, during a 2018 visit to Las Vegas, the FBI cornered him. He was kept in a hotel

---

[4] Diego Gambetta, *Codes of the Underworld: How Criminals Communicate* (2011).

[5] *See, e.g.,* Joseph Cox, *How Police How Police Secretly Took Over a Global Phone Network for Organized Crime*, VICE (July 2, 2020), https://www.vice.com/en/article/how-police-took-over-encrochat-hacked/.

[6] Jon Fingas, *Dutch police seize a secure communications network,* ENGADGET (Apr. 24, 2016), https://www.engadget.com/2016-04-24-dutch-police-seize-secure-communications-network.html.

[7] Joseph Cox, *Inside the Phone Company Secretly Run By Drug Traffickers*, VICE (Oct. 22, 2019), https://www.vice.com/en/article/wjwbmm/inside-the-phone-company-secretly-run-by-drug-traffickers.

[8] Phantom Secure was not the only encrypted phone company that leveraged a modified version of a mass-market device. A rival firm named beStealth that catered to a particular gang in Canada set up its own BlackBerry Enterprise Server where it controlled the encryption key. DARK WIRE, *supra* note 1, at 24.

room for several days while the FBI sought to cut a deal for access to the Phantom Secure servers. The CEO escaped, however, shutting down the company's servers while making a run for Canada. He was captured just short of the border because of his purchase and use of a prepaid "burner" phone—which, ironically, he expected to be secure—to contact executives of his company. More specifically, the FBI obtained the phone number of the burner phone when the CEO used it to contact other Phantom Secure executives. The FBI then followed the phone as it pinged cell towers on the way towards Canada. The CEO was captured just short of the border when he stopped to get lunch.[9] Phantom Secure then shut its operations down permanently. Reports on its user base vary, but the FBI estimated Phantom Secure had around 20,000 users at the time.[10]

The user estimates for Ennetcom, MPC and Phantom Secure are rather striking in that they are quite low when compared to mass-market encrypted communications apps like BlackBerry Messenger, Telegraph, WhatsApp or Signal, which had tens or hundreds of millions of users, of whom presumably the great majority are not engaged in criminal activity. For an antitrust practitioner, this raises the question of whether there are identifiable consumers that want specialty hardware/software solutions so much that they constitute an antitrust market? In other words, if Ennetcom, MPC and Phantom Secure had merged, could they have raised prices by a small but significant amount without precipitating an unprofitable shift of use to BlackBerry Messenger, Telegraph and other mass-market commercial options?

From the perspective of an antitrust economist, this can be seen as a hope that there was an antitrust market for dedicated devices enabling encrypted communications, which the FBI wanted to monopolize.

Although police and federal law enforcement agencies like the FBI do not normally concern themselves with hypothetical monopolist tests, this was nonetheless an important question for law enforcement. When they breached, or shut down, one encrypted phone company, what competitive alternative did criminal users have, and could law enforcement follow them to their new communications solution? Or, even better, could the FBI and law enforcement get ahead of the problem and offer criminals a place to go that law enforcement already controlled?

For this strategy to truly succeed, there would have to be significant substitution between the products, i.e., the FBI-controlled product would be the closest substitute for the soon-to-be-shut-down products, thus shutting down rivals would move the great majority of criminal traffic onto an FBI-controlled network. From the perspective of an antitrust economist, this can be seen as a hope that there was an antitrust market for dedicated devices enabling encrypted communications, which the FBI wanted to monopolize. Of course, any amount of diversion would still mean criminals whose communications the FBI would have complete access to, but, all else equal, the more criminals diverted the better.

A Story of Market Entry: FBI Development of Anom

After the failure to flip the Phantom Secure CEO, the FBI was approached later in 2018 by an app developer with an audacious plan. This developer had been getting ready to launch his own encrypted phone service. Concerned about his legal exposure if he proceeded, he proposed that instead *the FBI* develop, launch and manage the product. Doing so involved significant legal

---

[9] Dark Wire, *supra* note 1, at 64-65. *See also* Press Release, U.S. Dep't of Justice, Chief Executive and Four Associates Indicted for Conspiring with Global Drug Traffickers by Providing Encryption Services to Evade Law Enforcement and Obstruct Justice (Mar. 15, 2018), https://www.justice.gov/usao-sdca/pr/chief-executive-and-four-associates-indicted-conspiring-global-drug-traffickers ("This is the first time the U.S. government has targeted a company and its principals for knowingly and intentionally conspiring with criminal organizations by providing them with the technological tools to evade law enforcement and obstruct justice while committing transnational drug trafficking.").

[10] Press Release, FBI, International Criminal Communication Service Dismantled (Mar. 16, 2018), https://www.fbi.gov/news/stories/phantom-secure-takedown-031618.

questions, but the FBI resolved those questions to its satisfaction. In brief, the FBI worked out an arrangement where data gathered abroad during the operation would go to the law enforcement agency of a third party country, which would—in most cases—then provide the data to the FBI.[11] The sting was on. The product would be called Anom.

The FBI was deliberately trying to develop a product that would attract criminals—and only criminals. Furthermore, the FBI needed a product and feature set that its consumers would think was functioning in the way intended and doing well enough to be an attractive product to criminals, but not to non-criminal consumers, but was also actually doing the opposite of what was claimed in terms of security and data privacy without that deception being easily detectable.[12] As one FBI agent noted, "[n]o one would actually use Anom if it were an inferior product."[13] The product itself consisted of two parts: 1) an Android device running a customized operating system, and 2) the encrypted messaging app itself, called Anom.

On the software side, the FBI began with a well-regarded open source security-oriented operating system called GrapheneOS. They modified it into their own operating system called ArcaneOS. This was installed onto Android phones.[14] Although GPS was not physically disabled as in Phantom Secure's phones, Anom marketed that its ArcaneOS shut off GPS. That was not true. In fact, not only was an Anom phone's GPS not shut off, but the Anom app automatically attached precise latitude and longitude to every message before transmitting it to law enforcement.[15] Anom also marketed that its servers were located outside of the EU and the Five Eyes alliance countries (US, UK, Australia, NZ, Canada), thus making it more difficult for enforcers to access them.[16] Of course, the servers were in fact controlled (indirectly) by the FBI. And it appears that at least some of the servers were, in fact, located in Five Eyes alliance countries.

Handset production was originally done at a single facility under the FBI's control in Hong Kong, using inexpensive or refurbished phones.[17] Later, as production ramped up, literal black boxes were used to install the operating system and the Anom app. As discussed later, the tools of production were eventually stolen and then cloned by distributors during fights among distributors for control of particular geographic markets.

The Anom messaging app itself had a variety of functions. To begin with, the app was hidden behind what looked like a calculator. You typed a passcode into the calculator and the messaging app would come up.[18] Other (claimed) functionality was added over time based on requests from customers, sometimes copying popular features from apps like WhatsApp.[19]

---

[11] Dark Wire, *supra* note 1, at 107-14.

[12] That is, the FBI wanted product characteristics that would not be of interest to "civilians," or at least should not be marketed to "civilians." More on this later, but in economic terms, the FBI wanted a supply chain that would market exclusively to criminals and not to "civilians," and also to have a feature set that would be demanded disproportionately by criminals and not particularly attractive to civilians. The latter is particularly challenging.

[13] Dark Wire, *supra* note 1, at 81.

[14] *Id.* at 96-97.

[15] *Id.* at 119-120.

[16] *Id.* at 95. Five Eyes is short for the Five Eyes Intelligence Oversight and Review Council (FIORC), which is composed of intelligence agencies from five Anglospheric countries. *See* U.S. Office of the Director of National Intelligence, Five Eyes Intelligence Oversight and Review Council (FIORC), https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc.

[17] Dark Wire, *supra* note 1, at 99.

[18] *Id.* at 96.

[19] *Id.* at 118.

Raising Rivals' Costs and Attempted Monopolization

Unlike firms operating in aboveboard markets, the FBI could help Anom succeed by degrading or destroying its competitors—"raising rivals' costs."

Setting up Anom was an achievement in and of itself. The FBI and its partners lacked experience running an encrypted phone business (or, really, any start-up). Once established, Anom pursued an objective just like a rational profit-seeking firm would; it was just that Anom sought to maximize information acquisition from a particular group of customers—criminals—as opposed to profits.

To do this, the FBI needed to compete "on the merits" by offering a product that at least was perceived as delivering higher value than its competitors. Unlike firms operating in aboveboard markets, the FBI could help Anom succeed by degrading or destroying its competitors—"raising rivals' costs." The FBI had tools available to destroy or degrade its competitors that went well beyond what antitrust economists might normally see. That is, the FBI and its various international law enforcement allies could potentially speed adoption of Anom by diminishing the quality, or even viability, of competitors by directly expropriating their assets and imprisoning their executives. As noted in *Dark Wire*: "[W]hat if law enforcement knocked out Anom's competition in the secure phone industry? If the FBI closed down Sky [another encrypted phone service] entirely, like it had with Phantom Secure, those customers wouldn't just call it quits and go home. They would find a new provider. Lying in wait to happily take on those clients would be Anom."[20]

Two of the larger encrypted phone providers that competed with Anom were Sky and Encrochat. Both were shut down by enforcers while Anom was operating, providing natural experiments as to diversion rates.

According to Europol, "EncroChat phones were presented to customers as guaranteeing perfect anonymity (no device or SIM card association on the customer's account, acquisition under conditions guaranteeing the absence of traceability) and perfect discretion both of the encrypted interface (dual operating system, the encrypted interface being hidden so as not to be detectable) and the terminal itself (removal of the camera, microphone, GPS and USB port)."[21] EncroChat sold its 1000€ phones internationally, and offered subscriptions and 24/7 support.[22] Unfortunately for EncroChat users, the French police had taken over an Encrochat server in France and used it to push malware onto Encrochat phones. As explained in *Dark Wire*, "Encrochat users felt something was wrong but couldn't put their finger on what. In pockets of Europe, the police pulled gang members off the street. The cops seems to be everywhere the criminals turned. . . . [Users] complained to Encrochat, who started to investigate."[23]

EncroChat obtained one of the impacted phones in June 2020 and discovered the French police's malware. EncroChat pushed an update to customers' phones within 48 hours, but ultimately closed itself down the same month.[24] At that time, EncroChat had about 60,000 users.[25]

---

[20] Dark Wire, *supra* note 1 at 77.

[21] Press release, Europol, Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe (July 2, 2020), https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

[22] *See* Press Release, Europol, Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe (July 2, 2020), https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

[23] Dark Wire, *supra* note 1, at 143.

[24] *Id.* at 144.

[25] Reuters, *Encrypted phone service 'Encrochat' shutdown leads to 6,500 arrests, Europol says* (June 27, 2023), https://www.reuters.com/world/europe/encrypted-phone-service-encrochat-shutdown-leads-6500-arrests-europol-2023-06-27/.

Like EncroChat, Sky ECC "bill[ed] itself as the 'most secure messaging platform you can buy' and [was] so confident of the impregnability of its systems that it offer[ed] a handsome reward for anyone who [could] break the encryption of one of its phones."[26] It offered a feature set similar to Anom's claimed feature set, including self-destructing messages, group chat, ability to hide the app as a calculator, and a secure vault for on-phone storage.[27] Sky ECC ensured that, on the handsets it provided, all apps were blocked except its own app, and the handset could only be used to communicate with other Sky ECC phones.[28] One additional feature was that if the phone was not accessed properly in a certain period of time, the phone would erase itself.[29]

Notwithstanding Sky's promises of impregnability, European enforcers ultimately were able to access communications for some, but not all, Sky ECC users—about 70,000 of them.[30] This became public in February 2021, and Sky ECC shut its servers down shortly thereafter.[31] Sky ECC had about 170,000 users worldwide.[32]

The sudden endings of EncroChat and Sky ECC provide natural experiments as to diversion and market definition. Data are sparse, but the results may be surprising, depending on whether one shares the FBI's priors about (criminal) consumer preferences.

When discussing the ending of EncroChat and Sky ECC, it is important to know that Anom itself was shut down in June 2021—a voluntary decision by enforcers, but one driven by legal considerations (e.g., the Lithuanian court order providing for transfer of the traffic to the FBI was expiring in June[33]), as well as increasing suspicions and revelations about Anom's covert activities. Here is a brief timeline:

2016	• Ennetcom shuts down, with about 19,000 users
2018	• Phantom Secure shuts down, with about 20,000 users • Anom begins beta testing in Australia
2019	• MPC shuts down, with about 5,000 users • Anom reaches a few hundred users
2020	• EncroChat shuts down in July, with about 60,000 users • Anom reaches about 3,000 users
2021	• Sky shuts down in March, with about 170,000 users • Anom shuts down in June, with about 12,000 users

[26] Bill Goodwin, Computer Weekly, *Police crack world's largest cryptophone network as criminals swap EncroChat for Sky ECC* (Mar. 10, 2021), https://www.computerweekly.com/news/252497565/Police-crack-worlds-largest-cryptophone-network-as-criminals-swap-EncroChat-for-Sky-NCC.

[27] Mathew Schwartz, Bankinfo Security, Police Target Criminal Users of Sky ECC Cryptophone Service (Mar. 11, 2021), https://www.bankinfosecurity.com/police-target-criminal-users-sky-ecc-cryptophone-service-a-16162.

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Dark Wire, *supra* note 1, at 237-239. *See* Press Release, U.S. Drug Enf't Admin., Sky Global Executive and Associate Indicted for Providing Encrypted Communication Devices to Help International Drug Traffickers Avoid Law Enforcement (Mar. 21, 2021), https://www.dea.gov/press-releases/2021/03/12/sky-global-executive-and-associate-indicted-providing-encrypted.

[32] *See* Press Release, Europol, New major interventions to block encrypted communications of criminal networks (Mar. 10, 2021), https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks. Some news reports indicated total users were 70,000, but per the Europol news release, the 70,000 figure referred to the number of users that the enforcers were able to monitor, not the total number of users on the service. *Id.*

[33] Dark Wire, *supra* note 1, at 272.

In economic terms, the FBI's incentives were to maximize output (usage of its phones by criminals) and not profits.

The first item of note is that when EncroChat shut down, few customers went to Anom. Most went to Sky. "Ultimately, Sky became the de facto replacement for Encrochat in many places, not Anom."[34] This was not for lack of trying on Anom's part. After Encrochat shut down, Anom pushed sales in Europe. A Sky subscription could cost $1k and $2k for six months. Anom promotions ran as little as $600, and distributors sometimes gave phones away for free. "Worry about the money later, and take as many as you want. Just hand out the phones to your people, [one distributor] told his gangster contacts."[35] In economic terms, the FBI's incentives were to maximize output (usage of its phones by criminals) and not profits. But even with very aggressive pricing relative to Sky, it appears diversion to Anom was quite limited.

Sky was shut down next. *Dark Wire* characterized the shutdown as "a purposeful, anticompetitive practice: unceremoniously kill the rival, and further monopolize the marketplace."[36] As after EncroChat's demise, Anom attempted to take advantage of the shutdown, ramping up production and deeply discounting its handsets.[37] There were only a few months between Sky's shutdown and Anom's shutdown, so it is possible that more diversion would have occurred over time, but it appears that relatively little happened in those months. Anom's sales did appear to increase, but only modestly.

Ultimately, between EncroChat and Sky, there were roughly 230,000 users up for grabs, yet Anom's users grew by only a few thousand after both of its rivals were driven from the market. This lack of diversion suggests that the FBI's attempt to monopolize a hypothesized market of encrypted hardware/software communications for a dedicated market of criminal users was, in antitrust terms, remarkably unsuccessful. There was too much diversion outside of the market.

Why was that? It appears Anom's deception may have been detected (or at least suspected) and publicized by rival suppliers.[38] Some customers self-supplied. For example, some simply bought their own phones, took out the camera and microphone, and threw the phone away after a month, buying a new phone to replace it.[39] Others presumably moved to encrypted apps, either mass market or more specialized, such as had previously been done with BlackBerry encrypted messaging.

It is also possible that there was some *Cellophane*-like effect going on. One of the purposes of these operations was to undermine trust in encrypted phone companies generally. Arguably, people burned once at EncroChat and Sky (or possibly multiple times if they had previously used other encrypted phone companies) might have chosen to substitute away from encrypted phones entirely because the expected quality of the phones was substantially lower in light of the repeated security breaches. That is, users that did not previously regard mass market apps or stand-alone specialized apps as close substitutes for an integrated hardware-software solution might have reconsidered that position in light of repeated security breaches of encrypted handsets. Whether this constitutes a win for law enforcement is a different question.

---

[34] *Id.* at 193.

[35] *Id.* at 154.

[36] *Id.* at 240.

[37] *Id.* at 241.

[38] *Id.* at 256.

[39] *Id.* at 310-311.

The Challenges of Distribution in an Untrusting Market

Anom's distribution process changed over time, illustrating several interesting economic phenomena. For example, encrypted phone companies went to market using a combination of direct sales and third-party distributors. In some cases, the companies, including Anom, would get senior leaders of existing criminal organizations to be distributors, offering them a financial stake in doing so, and sometimes an ownership stake. For example, a former Comanchero biker gang member got partial ownership of Ciphr that gave him exclusive distribution rights in Australia, i.e., control of that geographic market.[40] To an industrial organization economist, the relationships between phone companies and the gang leaders can be seen as an attempt to use contracts to align interests much as a franchisor might in legitimate industries. Enforcement of those contracts is another issue, as we see later.

Anom's distribution process changed over time. Originally, all Anom handsets were assembled in Hong Kong. While other companies would use combinations of direct sales and resellers, Anom was only sold through resellers because of the FBI and other law enforcers' concerns about possible entrapment defenses.[41] Getting an existing reseller to switch between phone companies could move thousands of customers with that reseller. For example, shortly before Anom was shut down, No. 1 BC (another encrypted phone company) lost to Anom a reseller who had an alleged customer base of 10,000 users, although it appears Anom was shut down before that resulted in any notable Anom sales.[42]

The idea that a reseller could, in fact, move customers between products also suggests that resellers may have had a vetting role—customers might trust a reseller to vet the various products on the market, and to have more expertise in doing so than the customers themselves. Resellers may also have had incentives to do a good job on vetting, as expressions of customer dissatisfaction could go well beyond a sternly worded letter. That is, a reseller with dissatisfied customers could be physically assaulted or killed. These are examples of how economic actors may align incentives when they do not have access to the legal system to enforce contracts and consumer protections.

As Anom scaled up, production changed to accommodate increased demand for its handsets. When EncroChat shut down, only one non-FBI person (a reseller in the Dutch city of Nijmegen) had been provided a black box to create Anom handsets.[43] This number grew as demand for Anom expanded. Anom also created a web portal through which resellers could activate phones, where previously Anom would have to activate each phone individually.[44]

Anom itself was not establishing or enforcing sales territories for its different resellers, and this gave rise to disputes. One distributor that had a network of resellers "likened the selling of phones to having a drug territory: if someone else on his or his resellers' turf sold encrypted phones, he suggested sending someone to shoot them."[45] This particular distributor stole the black box in

---

[40] *Id.* at 125. It is an open question as to whether any given area constituted a geographic market in an antitrust sense, but the competition for control of distribution channels in a given geographic area is suggestive.

[41] *Id.* at 157.

[42] *Id.* at 277.

[43] *Id.* at 230-231.

[44] *Id.* at 232.

[45] *Id.* at 156.

Nijmegen, and also stole black boxes from other resellers.[46] He succeeded in taking over distribution from rivals in various countries, again suggesting that there were geographic markets that distributors competed over.

Eventually, Anom's customers worked out how to clone the black boxes, further opening up the distribution process.[47] Quality fell, as the people now using the black boxes were not properly trained in their use.

Distributors had no incentive to think about the spillover effects that shirking on quality would have on demand overall.

To an economist, the proliferation of black boxes and lower costs of entry to resellers would give rise to offsetting effects. On the one hand, the proliferation of distributors and resellers increased intra-brand competition, which could lead to increased adoption of the product itself. On the other hand, there was no central quality control as to the handsets themselves, their programming, or their labeling. Distributors had no incentive to think about the spillover effects that shirking on quality would have on demand overall. This is a form of the tragedy of the commons. Phones would go out not properly programmed or incorrectly labeled.[48] Distributors would use lower quality phones that could not even run the ArcaneOS, and would only have the Anom app.[49] In some cases the Anom phones wouldn't work at all. One anecdote involved a gentleman getting out of prison, obtaining an Anom phone, and having it fail right out of the box.[50] A "fly by night" distributor would not care about the impacts on the overall brand, although, as noted, resellers had to be aware that at a certain point quality concerns might result in customers taking enforcement action of their own.

At the end of the day, an illegal business is still a business. The inability to enforce contracts through the legal system represents a problem if incentives are not perfectly aligned, leading to the use of alternative enforcement mechanisms such as peer pressure, violence, or financial incentives. And, of course, illegal competition tactics such as robbing your competing distributors or literally destroying their facilities are on the table. Unlike the FBI's efforts to monopolize the product market, individual distributor efforts to seize and hold exclusive distribution in various geographic markets appear to have been more successful, in large part because of their ability and willingness to resort to theft and violence.

Control of distribution could be a thorny issue from the FBI's perspective. Anom wanted as much as possible for its handsets to be in the hands of criminals, and only criminals. Using resellers targeted at criminals was a way to do so, as was trying to offer features tailored to attract criminals. But non-criminal groups have interests in encrypted communications as well. Sky, for example, argued that it was not deliberately marketing to criminals, but that unauthorized resellers were selling its products to criminals. Unlike Anom, Sky did not exclusively use resellers but also had direct sales—one could buy Sky phones off of their website.[51] And Sky in fact claimed to work to get criminals off its platform by banning resellers selling to criminals. However, resellers would use pseudonyms to avoid being cut off.[52] One former Sky employee said that Sky knew bad people used the phones, just like bad people used Signal or WhatsApp. Enforcers argued that Sky

---

[46] *Id.* at 233.

[47] *Id.* at 245.

[48] *Id.* at 233.

[49] *Id.* at 242.

[50] *Id.* at 280.

[51] For a screenshot of the Sky website sales page, *see* Schwartz, *supra* note 27.

[52] Dark Wire, *supra* note 1, at 74-75.

was qualitatively different from mass-market encryption services because it sold premium-priced phones as opposed to free to download apps widely used by the general public.[53] In economic terms, enforcers were arguing that the pricing differential indicated that the mass-market products were in a different antitrust market, and that the consumers in the high-priced market were primarily criminals, not the general public. The approach appears to have been largely—but not perfectly—successful for Anom.

Conclusion

It is interesting that in spite of all of its advantages, Anom was unable to obtain a particularly large share of criminals' encrypted communications. Even when larger rivals were literally shut down overnight, the great majority of those users went elsewhere. This all suggests that monopolizing a market can be quite challenging even when one is unfettered by antitrust laws because, as Project Trojan Shield demonstrates, antitrust economics apply to criminal enterprises. That takeaway, and the intriguing path to arrive at it, makes *Dark Wire* a worthwhile diversion for economists, antitrust lawyers, and true crime afficionados alike. ●

This all suggests that monopolizing a market can be quite challenging even when one is unfettered by antitrust laws because, as Project Trojan Shield demonstrates, antitrust economics apply to criminal enterprises.

[53] *Id.*