Name of organization: ELECTRONIC PRIVACY INFORMATION CENTER

Employer identification number: 52-2225921

**Part II Noncash Property** (see instructions). Use duplicate copies of Part II if additional space is needed.

| (a) No. from Part I | (b) Description of noncash property given | (c) FMV (or estimate) (See instructions.) | (d) Date received |
|---|---|---|---|
| 4 | XRP CRYPTOCURRENCY | $ 1,000,000. | 03/15/19 |

# How Watchdogs are Silenced

## As the U.S. contemplates the creation of an intelligence agency modeled after Bellingcat, the failure mechanisms of civil society become even more relevant. A year-long Tech Inquiry investigation reveals how even Amnesty International partnered with Palantir's "beta test-bed".

**Jack Poulson, Tech Inquiry, 2023-03-06**

***[2023-03-06, 1:00pm ET] A reference was added to Citizen Lab's John Scott-Railton having similarly refused to comment to Motherboard on which facial recognition he employed on January 6th rioters.***

Employees and advisors of former Google CEO Eric Schmidt's national security think tank, the Special Competitive Studies Project (SCSP), are campaigning for the creation of a new "open source" intelligence agency modeled after the investigatory nonprofit Bellingcat. SCSP's Intelligence Director, Peter Mattis, recently used his credentials as a former CIA counterintelligence analyst to help make the case in an op-ed in The Hill alongside former CIA intelligence officer Rodney Faraon.

SCSP Advisor Amy Zegart, who is also a board member of a military drone manufacturer, argued in the most recent episode of SCSP's podcast that such a 19th intelligence agency is necessary if the U.S. is to keep pace with nations which learn to nimbly incorporate information from unclassified sources. Zegart went on that such an open source agency would "flip the script" on the myriad siloed components of the 18 existing U.S. intelligence agencies (of which the CIA, FBI, and NSA receive by far the most public attention).

To some degree “open source” is a marketing term —the practice regularly involves the usage of large-scale facial recognition, social media surveillance, and, in many cases, non-consensual cell-phone location tracking. In military contracting circles, “Publicly Available Information” is often the preferred term of art instead of “Open Source Intelligence”, or “OSINT”. (The term “Commercially Sourced Intelligence”, or “CSINT”, is also advocated by some former CIA executives to distinguish commercially purchasable data from that which can be freely downloaded from the open internet.)

Perhaps the most famous example of public outcry against “open source” / “Publicly Available Information” surveillance is in regards to the facial recognition firm Clearview AI; the company has been fined and/or banned in numerous countries for its nonconsensual automated downloading of billions of faces and names from websites such as Facebook (which it then resells to police around the world). Yet the connotations of “open source” intelligence are still largely positive, even for organizations which openly employ facial recognition from Clearview AI’s competitors.

Open source intelligence nonprofits such as Bellingcat and its colleagues Citizen Lab and Center for Advanced Defense Studies (C4ADS) have become the go-to sources in foreign policy reporting: Citizen Lab largely plays the role of civil liberties watchdog and spearheaded a global campaign to ban the Pegasus phone-hacking software; Bellingcat is widely cited for its dogged usage of facial recognition and satellite imagery to investigate Russians; while C4ADS is known for its skill in investigating the avoidance of U.S. sanctions through its high-tech platform combining corporate registry and location-tracking datasets. (C4ADS’s Executive Director, Special Forces veteran David Johnson, has described the platform as a “beta test-bed” for the data fusion company Palantir, which has been mired by international human rights concerns over its support for drone warfare and immigration enforcement since its founding.)

The central question driving this reporting is when and how friendships, board positions, and the plausible deniability of nonprofit intermediaries lead to watchdogs transforming from publicly rebuking surveillance firms to instead partnering with — or pointedly refusing to comment on — close affiliates of the same firms. ***The point of this inquiry is to expose the influence of corporations through the vehicle of nonprofits; the unavoidable spectacle of the hypocrisy of said nonprofits is arguably a distraction from the corporate influence itself.***

Tech Inquiry has repeatedly encountered instances of even the most revered privacy and human rights watchdogs flipping into protectors of corporate interests and surveillance — indeed we have documented surprising instances of our own small organization being pressured to do the same. Prominent cases include how Citizen Lab and Democracy Now! respond to the deployment of facial recognition, that Amnesty International partnered with the de facto think tank arm of Palantir and long sought to obscure the relationship, and the manner in which the Electronic Privacy Information Center hides the sources of even million dollar cryptocurrency donations and ignores the surveillance relationships of the corporate executives on its governing and advisory boards.

## Crisis Text Line, EPIC, and Ripple Labs

POLITICO reported in January 2022 that the non-profit Crisis Text Line had created a for-profit spin-off named Loris.ai to monetize the conversations it had collected with vulnerable individuals through its suicide helpline. The investors of Loris.ai — which include progressive bulwark Omidyar Network and a venture capital firm founded by one of the creators of privacy vanguard Electronic Frontier Foundation — were affiliated with precisely the watchdogs one would expect to oppose such privacy abuses. Loris.ai's exploitative business model had been openly promoted at a 'Talk at Google' in June 2019 and was long critiqued through the website of whistleblower Tim Reierson, yet the watchdogs had remained silent.

One of the most respected members of the tech privacy and ethics community — Microsoft Partner Researcher danah boyd — had become president of Crisis Text Line in June of 2020 in addition to their then role as President of the think tank Data & Society, which was founded in 2014 by "a generous gift from Microsoft". In response to public critique, boyd admitted in a blog post that she had formally voted for the monetization of Crisis Text Line's conversations with vulnerable individuals to "*leverage empathy*". boyd's long-time friend, tech ethics thought leader, and pop-up ad creator Ethan Zuckerman quickly came to her public defense, speculating that boyd was legally constrained from explaining the reality of the situation and stating that he had "*a great deal of respect for danah*" for staying on the board to fix it from the inside.

Beyond Zuckerman's public defense of his friend, perhaps the second-most influential privacy watchdog after the Electronic Frontier Foundation, the Electronic Privacy Information Center (EPIC), continued to endorse boyd as a member of its advisory board. In response to an inquiry from the author as to the propriety of retaining an advisor who has admitted to behavior antithetical to the mission of EPIC, Executive Director Alan Butler stated that "*danah boyd is one of the leading experts on differential privacy and her advice on issues related to privacy enhancing techniques and sociological issues relating to use of technology continue to be an important resource informing EPIC's privacy research.*"

And despite the embattled Chairman of cryptocurrency firm Ripple Labs, Chris Larsen, being an advisor and, until recently, long-time board member of EPIC, Butler continues to refuse to state whether EPIC's March 15, 2019 receipt of a million dollars of Ripple's XRP cryptocurrency originated from Larsen. Butler justified his refusal on the grounds that EPIC "*protect[s] the privacy of our donors*" and argued that EPIC "*do[es] not accept corporate sponsorships, contracts, fellowships, or research funds*", but that Larsen voluntarily disclosed his sponsorship of numerous EPIC events.

Beyond the Chairman of the sixth largest cryptocurrency bankrolling and helping to govern one of the most respected privacy watchdogs while under active SEC investigation, Ripple Labs is a central member of an international collection of cryptocurrency lobbying groups which includes the Digital Pound Foundation, Blockchain for Europe, the Chamber of Digital Commerce, and the Digital Euro Association.

Ripple Labs did not respond to a request for comment.

(After the U.S. indictment of former cryptocurrency billionaire Sam Bankman-Fried (SBF) for conspiracy to commit wire fraud, commodities fraud, securities fraud, and money laundering, the numerous multi-million dollar donations from SBF to vaunted nonprofit media outlets such as ProPublica and The Intercept became the subject of public scrutiny. ProPublica announced that it would return the donation in December 2022, but, as of one week ago, The Intercept has characterized the $4 million grant as 'suspended' rather than promising a return or redirection of the $500,000 received so far.)

And in a recent interview with Bloomberg regarding the SEC's ongoing investigation into whether Ripple misled its investors and failed to register its digital assets as a security, the CEO of Ripple claimed that the United States is falling behind other countries as a result of its overregulation of cryptocurrency. (Butler clarified for Tech Inquiry this week that Larsen voluntarily stepped down from EPIC's board and remains eligible to return.)


A screenshot of entity-resolution company Senzing's partners and customers which lists surveillance and weapons contractor Lockheed Martin as well as border security social media surveillance contractor Giant Oak.

Butler further refuted concerns that EPIC board member and CEO of entity-resolution company Senzing was profiting from government surveillance as a result of his company's subcontracts with the U.S. Air Force through the non-profit government research lab MITRE or from the company's public partnerships with weapons and surveillance contractor Lockheed Martin and social media surveillance firm Giant Oak. (Giant Oak has been widely criticized for selling its social media surveillance services to U.S. immigration and border enforcement agencies; Jonas describes entity resolution as the process of resolving when two different variations on the spelling of a name refer to the same entity — which has clear implications for military and law enforcement analysis of social media.)

Senzing did not respond to a request for comment.

## Citizen Lab and Bellingcat's caveated-promotion of facial recognition

Journalist Jacob Silverman noted two years ago in The New Republic that civil society investigatory organization Citizen Lab, which is widely respected for the quality of its research into the human rights abuses in the surveillance industry, had responded to the January 6th riot by flipping from criticizing facial recognition to instead employing it in on rioters in collaboration with the FBI. (The investigation was prominently featured in an article in The New Yorker.)

When reached for comment by Tech Inquiry, Citizen Lab's Director Ronald Deibert refused to clarify what facial recognition software or facial datasets had been used by its senior researcher John Scott-Railton (who did not respond to requests for comment). Citizen Lab has closely partnered with Microsoft in the past, but freely available facial recognition from sites such as PimEyes is equally as likely. Deibert pointed to his past critique of the controversial — and seemingly failing — facial recognition firm Clearview AI and stated that Citizen Lab's usage of facial recognition was "one-off" but would not comment on whether the organization regretted its endorsement of facial recognition or its collaboration with the FBI.

(Scott-Railton similarly refused to comment to Motherboard in February 2021 on which facial recognition he used.)

Like Citizen Lab, Clearview AI quickly began working with the FBI to identify the January 6th rioters using facial recognition — but Clearview AI's arguable motive was in countering lingering associations with the far-right resulting from its founding. And while the company's leaked December 2021 pitch deck and January 2022 open letter argued Clearview AI's facial recognition is a crucial component in the United States's technological battle against Russia and China, the company responded to Russia's February 2022 invasion of Ukraine with a full-scale marketing campaign emphasizing how the government of Ukraine has used Clearview AI to surveil Russians.

In the months following the invasion, the most publicized open source intelligence nonprofit, Bellingcat, promoted its usage of a Russian analogue of Clearview AI called FindClone to identify Russian soldiers and investigate alleged Russian spies.[1] The primary difference between the two programs is that, while Clearview AI scrapes essentially all popular social media sites — including Facebook — FindClone focuses on the Russian Facebook competitor VK.

Bellingcat's director or research and training, Aric Toler, described to Slate how his organization's usage of FindClone allows them to find alleged Russian intelligence agents through photos posted by their family members: "w*e do a lot of work with Russian spies and security service officers, people who don't usually have accounts. But their wives do. And their old college buddies do, and their brothers do, and their moms do, and their kids do. You'll find them in the background of photos at a birthday party they had, you can see their face behind a cake.*"

But Toler argued that Clearview AI had gone too far by boasting of its harassment of the mothers of deceased Russian soldiers and told Tech Inquiry that Bellingcat had refused Clearview AI's offer to use their product, partly in response to Clearview AI "*offer[ing] their services to police departments and security services around the world*".

When asked about Bellingcat being proposed as the model for a new "open source" U.S. intelligence agency, and whether the group had concerns about becoming the justification for U.S. intelligence agency usage of facial recognition, Toler told Tech Inquiry that "*we're far from the only people using facial recognition for research. Russian independent media outlets were using it in very interesting investigations before we ever got a Findclone login…I guess we're just a brand name attached to the practice now because these people lobbying for more intel funding/agencies have heard of us.*"

Toler also argued that "*US security agencies have already been using Findclone for a while*" and pointed to his series of tweets from October 2020 asserting that "*the FBI 100% used Findclone*" in its indictment of six Russian intelligence agents.

When asked about Bellingcat's promotion of facial recognition for use on Russians, Citizen Lab's Deibert stated that he "*appreciate[s] the work [Bellingcat does] and I'm guessing they have some rationales one way or another.*"

Amnesty International refused to comment specifically on Citizen Lab and Bellingcat's usage of facial recognition but noted that the technology "*is incompatible with fundamental human rights, such as the right to privacy, equality and non-discrimination, and freedom of expression and peaceful assembly.*"

---

[1] Bellingcat has also frequently promoted its usage of Microsoft Azure's facial verification service but emphasized that the service is fundamentally different from facial search, stating that Azure's facial recognition API is a 'rudimentary' tool used as secondary evidence of whether two pictures are of the same person.

Seemingly as a result of the prestige of influential open source groups, civil liberties watchdogs ignore their colleagues high-profile descriptions of their deployment of facial recognition on the scraped social media accounts of the spouses and children of their targets. Civil society regularly speak out on Clearview AI's large-scale scraping of American and European social media accounts, but nonprofits adopt a more muted posture on — and many make use of — equivalent surveillance of citizens in countries run by U.S. adversaries.

Each organization justifies its own usage of facial recognition by that of its peers — presumably partially motivated by the need to stay relevant.

## Amnesty's partnership with a 'Palantir-powered' think tank

In 2006 when Christopher Darby was announced as the new CEO of the primary venture capital arm of the U.S. Intelligence Community — In-Q-Tel, Inc. — he was both a Vice President at chip manufacturer Intel and a senior fellow at then-obscure national security think-tank Center for Advanced Defense Studies. CADS, as it was then known, would later switch its acronym to C4ADS and become a collaborator with Bellingcat and the go-to source for high-profile coverage relating to sanctions on official U.S. adversaries such as China, Russia, Iran, and North Korea. (According to an ostensible copy of the center's "Inside the Tank" newsletter", Darby was also the vice chairman of the think tank under founder Newton Howard.)

C4ADS's conflicts of interest resulting from close funding and leadership relationships to U.S. intelligence and special operations are generally omitted when the organization is cited for its expertise on U.S. sanctions or the human rights abuses of U.S. adversaries. But a public audit reveals that roughly 89% of C4ADS's 2021 revenue came directly from the U.S. federal government, including a grant from the U.S. State Department's Bureau of International Security explicitly for "*Countering America's Adversaries Through Sanctions Act Section 231*".

C4ADS's website states that it "leverages" the controversial data fusion company Palantir "*to integrate manage, and utilize its data at scale*", while C4ADS's Executive Director, former Special Forces veteran David Johnson, has referred to C4ADS as a "*beta test-bed for a company called Palantir*". The two organizations also released a video explaining their partnership, and several C4ADS employees have recently moved to Palantir. One of them — former C4ADS Program Manager Jason Arterburn — has simultaneously been a C4ADS Fellow and a Deployment Strategist at Palantir since December 2022.

In keeping with U.S. military and intelligence interests, C4ADS has listed Saudi Prince Fahd bin Abdullah Al Saud as a Fellow, previously appointed the founding director of the CIA's Center for the Analysis of Personality and Political Behavior to its board, and the current board chair is former U.S. Ambassador to Hungary April Foley.

As was previously noted by Tech Inquiry using public records analysis, C4ADS was paid $250,000 for "bulk datasets" as part of a contract involving the Defense Intelligence Agency and controversial cellphone location-tracking data broker X-Mode Social (which later renamed to Outlogic). Perhaps X-Mode's biggest controversy was its nonconsensual sourcing of cellphone location-tracking data from the popular Muslim prayer app Muslim Pro, which it then ostensibly resold to to the Defense Intelligence Agency.

Despite C4ADS's close relationship with U.S. intelligence and special forces, they were nevertheless announced as a partner in international human rights organization Amnesty International's "Corporate Crimes Hub" at a June 2021 event whose speakers included Secretary General Agnes Callamard. The Corporate Crimes Hub website emphasized usage of C4ADS's corporate registry tool Seamless Horizons and C4ADS's expertise in vessel and aircraft tracking as central to the partnership.


A flyer for the June 22, 2021 launch of Amnesty International's Corporate Crimes Project, whose partners included the Palantir "beta test-bed" think tank, C4ADS. Amnesty International's Secretary General, Agnes Callamard, was announced as the headline speaker.

Beyond C4ADS's Palantir ties, former C4ADS staffers Farley Mesko and Benjamin Power founded a for-profit company named Sayari with a focus remarkably similar to C4ADS's Seamless Horizons tool. In contrast to C4ADS's human rights rebranding, Sayari was publicly invested in by In-Q-Tel and public records demonstrate that it has contracted with the DEA, ICE, CBP, the Australian Department of Defence, Canadian Border Services, and U.K. Revenue and Customs.

While Amnesty International's head of its Corporate Crimes Hub, Montse Ferrer, would not explain on-record how the partnership with a U.S. defense and intelligence contractor started or ended, Ferrer would eventually state that the relationship ended a month after Tech Inquiry asked about C4ADS's extensive ties to Palantir and U.S. intelligence. After a sequence of requests which began in March 2022 and which culminated with a request for comment from Secretary General Agnes Callamard, Tech Inquiry received the following statement from Amnesty spokesperson Tom Mackey on Friday:

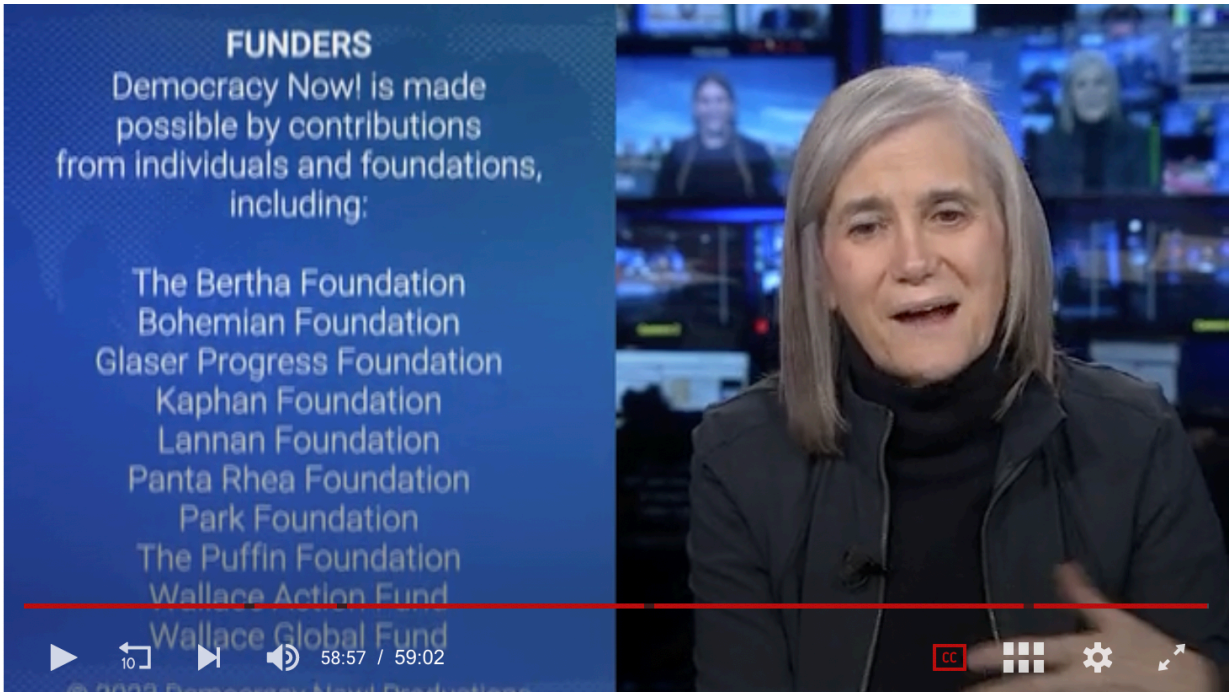
"*Amnesty International has raised serious concerns about Palantir's human rights record. When we became aware of C4ADS relationship with Palantir in March 2022, a review of C4ADS' involvement in the Corporate Crimes Network was undertaken. Following this review, C4ADS' involvement in the Corporate Crimes Network ended in April 2022.*"

Tech Inquiry has did not receive comment from Callamard, who was announced as the headline speaker for Amnesty's partnership with C4ADS et al. in June of 2021. Callamard is a revered human rights advocate who last month fiercely criticized the sanitized image of military contracting presented by the Dutch military through its REAIM Summit on the military applications of artificial intelligence. (Palantir CEO Alex Karp was hosted for a fireside chat at the same summit later the same day.)

## Democracy Now!'s connection to facial recognition for military drones

Tech Inquiry has spent more than a year asking for comment from the progressive newsroom Democracy Now! on whether it is aware that its prominent funder — Rob Glaser of the Glaser Progress Foundation — is the CEO of a major military facial recognition contractor, RealNetworks. RealNetworks has received millions of dollars over the past several years from the U.S. Air Force to specifically provide its facial recognition for use in U.S. drones and quadrupeds. Yet, despite repeated phone calls and emails — including directly to co-host Juan Gonzalez — the organization has refused to acknowledge receipt of Tech Inquiry's requests for comment. (Democracy Now!'s slogan is 'Go to Where the Silence Is'.)

While a funding relationship between a progressive newsroom which unambiguously opposes drone warfare and a company which sells facial recognition for use in military drones appears farcical at first glance, it begins to make sense when one understands the complicated history of RealNetworks. As detailed by investigative journalist Issie Lapowsky in 2018 for WIRED, RealNetworks was founded by Rob Glaser in the 1990s "*as a vehicle for broadcasting left-leaning political views*" — its name changed from "Progressive Networks" to RealNetworks in 1997 — and the company pivoted to selling its "SAFR" facial recognition product to schools (and later militaries) as a means of reinventing the struggling company.




A screenshot from the closing credits of Democracy Now!'s daily show for March 1, 2023 which clearly thanks the Glaser Progress Foundation — the non-profit arm of the CEO of facial recognition vendor RealNetworks, which has made millions through selling its facial recognition for use in U.S. Air Force drones and quadrupeds.

Glaser openly differentiates his facial recognition product based on his progressive credentials, including his previous membership on the boards of the Electronic Frontier Foundation and the foundation that publishes Mother Jones. Glaser also previously chaired and bankrolled the now-defunct Air America Radio — a progressive competitor to right-wing talk radio which helped launch the career of MSNBC host Rachel Maddow. One of Glaser's major selling-points for SAFR is that, unlike some of its competitors, the facial recognition is not coupled with ethnicity inference.

Much of the critical coverage of Clearview AI has focused on the far-right ties of its founders (such as Chuck Johnson) and investors (such as Peter Thiel), and it would appear that — on the flip side — much of the lack of media coverage of RealNetworks is due to its progressive roots. Clearview AI has received less than $100,000 in contracts with the U.S. Air Force according to current public records, while RealNetworks has received roughly $3.5 million (again, including explicitly for sales of its facial recognition for use in military drones).

## Tech Inquiry's own Relationship to Corporate Influence

The largest source of funds ever received by Tech Inquiry — roughly $50,000 — was a year-long contract to map out government cloud computing procurement with an international labor organizing affiliate of the Communication Workers of America (CWA) — which has undoubtedly been the most influential union in high-tech organizing over the past several years. As was previously reported, as a result of CWA's June 2022 neutrality agreement with Microsoft and Tech Inquiry's report concluding that Microsoft received significantly more money from governments than Amazon, Tech Inquiry was demanded by CWA's affiliate to remove all discussion of Microsoft or violate our organizational ethics and hide the funding source for the report.

The unexpected result of Tech Inquiry disclosing the CWA affiliate's request was a public denial from the affiliate that Tech Inquiry was requested to remove critique of Microsoft. We will state on the record for the first time here that our assertions are backed up by hours of audio recordings that began after the first request for Tech Inquiry to manipulate its report. (That there were audio recordings was already obvious to practicing journalists as a result of the highly detailed nature of the quotes in The Intercept's reporting.)

Tech Inquiry was also pitched by an existential risk nonprofit roughly one year ago on accepting a donation from cryptocurrency billionaire and Ethereum founder Vitalik Buterin which would be labeled as instead coming from the nonprofit. (Tech Inquiry declined.)

And as a matter of consistency as part of our investigations into conflicts of interest arising from corporate executives obtaining board seats in watchdog organizations: one of the previous board members of Tech Inquiry, Liz O'Sullivan, was invited to our board after blowing the whistle on the secretive Pentagon AI drone warfare contracting of her then employer, Clarifai. O'Sullivan subsequently (co-)founded a series of companies.

The first company was the "AI monitoring" company Arthur AI, which contracted with the Pentagon's Joint Artificial Intelligence Center "*to accelerate production AI capabilities across the Department of Defense (DoD)*". O'Sullivan subsequently became the CEO of Parity Technologies, Inc. (which recently rebranded to Vera), which has been involved in a series of legal disputes ultimately resulting in a split with the other major shareholder, the founder and former Twitter Director, Rumman Chowdhury. O'Sullivan now runs Vera, while Chowdhury operates Parity Consulting. As of the May 27, 2022 complaint, the dispute was O'Sullivan as CEO versus the rest of the company.

In terms of policy influence: O'Sullivan is currently a member of The National AI Advisory Committee (NAIAC), which advises the U.S. President on issues including "A.I. competitiveness" and the National AI Initiative. To date, no journalist has asked Tech Inquiry for comment on these matters. (Though WIRED has reported on the ostensible contradiction of Arthur's military contracting.)

## The conflict between coalition-building and accountability

Influential non-profits tend to have prestigious boards and — in the words of American sociologist C. Wright Mills — "*prestige is the shadow of money and power*". And given the open manner in which "open source" investigatory nonprofits are now being promoted by former CIA officers as models for a new U.S. intelligence agency, it is critical that the human rights concerns relating to the blending of civil society with intelligence agencies not be obscured by oversimplified narratives of valiant nonprofits opposing a handful of cartoonishly evil corporate actors.

One of the major forms of leverage within investigatory nonprofits and journalism is time and expertise: the well-trodden game of think tanks is to keep journalists satiated with exclusive access to deep expertise in exchange for favorable coverage of the think tank and its policy objectives. The same influence game of course plays a role in resource-constrained human rights organizations, who perhaps lack both the data access and analytical manpower available to corporate-backed nonprofits such as C4ADS. (One could plausibly argue that Tech Inquiry itself engages in this trade — though we would submit that our organization is so scrappy and poorly funded as to barely function.)

Tech Inquiry was only able to extract an on-record explanation from Amnesty International about why it ended its relationship with C4ADS after roughly a year of requests (which escalated to asking for comment from the Secretary General). Democracy Now! has, by contrast, continued to stonewall Tech Inquiry's requests for comment on its relationship to facial recognition for U.S. Air Force drones.

One of the potential benefits of the proposed open source intelligence agency was argued to be a blurring of the boundaries between tech companies, "open source" nonprofits, and U.S. intelligence. Ideally journalists would respond to the ensuing increase in conflicts of interests with a more critical treatment of the affiliated think tanks.

*The author, Jack Poulson, can be contacted by email at jack@techinquiry.org or through the end-to-end encrypted chat application Signal through +1.646.733.6810. For any sensitive inquiries, please use Signal on a phone which has never had your employer's software installed on it.*