Library Stack is an archive and publisher focusing on natively digital objects, which occasionally invites guest contributions in the form of a curated collection. In response to the first half of 2017, the editors presented their own cluster of software, typography, corporate publications, and purloined documents, all of which seemed to resonate at the present's frequency. Reality Winners was first published on June 18, 2017 at www.librarystack.org/reality-winners. With thanks to Mattathias Schwartz.

(Benjamin Tiven & Erik Wysocan, Eds.)

Cover: Go Rando (logo), Benjamin Grosser, www.bengrosser.com/projects/go-rando.

Voter fraud, Twitter bots, fake news, fake likes, alternative facts, false leaks, sock puppets, psychometrics. Shadow Brokers vs. Reality Winners. Consensual factuality has been replaced by a contentious arena of propositions and counter-punches; the once reliably "real" is now shot through with opaque personas, avatars, and profiles. Identity is under review by think tanks and policy institutes. Online space has become a full-time proxy war: unknown governments operating against (or with) unknown individuals for seemingly unknowable aims — all occasionally illuminated by anonymously leaked documents or the sudden surfacing of a whistleblower. Political professionals rush to cover any seam that becomes too visible, often choosing (rhetorically, at least) simply to opt out of reality itself. News unfolds rapidly (Leak! Testimony! Tweet! Attack! Counter-tweet!), somehow managing to feel both aleatoric and eerily scripted.

In the 1990s and early 2000s, asymmetric warfare — where large, formal state militaries are confronted by murky, small groups with improvised weapons and behaviors — dominated strategic discourse. Those years saw a lumbering American military face animal-borne IEDs (like exploding donkeys) in Iraq and Afghanistan, and the Israeli army laterally bulldoze inner apartment walls in densely occupied urban territories. But recently, a new mode of state-level conflict has replaced military asymmetries with social, cultural, and behavioral ones. It is said that we are now in the midst of "non-linear war" — the tactical manipulating of society's fragilities and norms to blur, confuse, and weaken an enemy, or achieve a geopolitical objective, without open conflict. Non-linear war aims to make other governments work less well, but not collapse; to claim authority over territories that had always been presumed international; to change future political stakes by inventing parties, issues, or actors where none had existed; to weaponize global flows of money and resources. It takes place across our softest interfaces — social media platforms, state television, YouTube memes, advertising— and occasionally concretizes into background threat levels or public demonstrations. It exaggerates contentious politics and in turn is helped by them. Non-linear war turns reality into an editing suite, where new combinations of cause and result are constantly being pieced together, focus-grouped, and reformulated if necessary. The objects in the following collection are artifacts of this ongoing process: moments where truth is distinguished from reality, value from price, language from meaning, emotion from feeling, and identity from Identity.

1. ART BASEL SUMMARY

Global art sales generated roughly $57 billion dollars in 2016, and here is a remarkable summary of its recent performance as an asset class by two key power players: a fair and a bank. The summary tells a story of segmentation and distension of the market towards extreme ends of the scale: a tiny fraction of artists make up the vast bulk of sales, with just .017% of galleries responsible for 80% of total sales by value. On page 236, the text suddenly worries about the effect of dramatic wealth inequality on the market, if chiefly in that it produces self-reinforcing feedback loops of nervous *nouveau-riche* collectors who buy only what already seems safe, thus tightening exclusive corners. With the recent boom years having crashed into the nativist politics of Brexit and Trump, art's peculiar contingency as a commodity becomes clear: the astronomical Return On Investment on a Warhol is only possible within a globalized marketplace.

www.librarystack.org/art-market-2017-the

2. DUBAI FONT

In late April, the Emirate of Dubai announced the release of its eponymous typeface, designed in conjunction with Microsoft and Monotype, which is both openly downloadable and bundled with Microsoft Office. A strikingly generic sans-serif built for some 23 languages, the typeface is designed to be easily read on any screen, at any size. It is marketed (in the dramatic language of too-serious PR campaigns) as simultaneously urban, global, ancient, and modern: it aims to synthesize Dubai's architectural futurism with heritage characters both Latin and Arabic. Like its namesake, the Dubai font wants to be anything for everyone — the Helvetica of capitalist universalism — able to knit together even civilizations that are otherwise at war, that they might at least still do business. The Dubai font is also vexingly marketed as a "new global medium for self-expression," which is ironic for a product of a repressive political climate.

www.librarystack.org/dubai-font

3. GO RANDO

In the words of its designer, artist Benjamin Grosser, Go Rando "is a web browser extension that obfuscates your feelings on Facebook. Every time

you click "Like," Go Rando randomly chooses one of the six "reactions" for you. Over time, you appear to Facebook's algorithms as someone whose feelings are emotionally 'balanced'"—that is, your profile becomes obscured by false emotional noise, and rendered less useful to Facebook's algorithms. Grosser notes that Facebook's "reactions" capacity enables and abets its expanding role in surveillance, government profiling, advertisement micro-targeting, and emotional manipulation across the platform. Short of leaving the service entirely, clouding its ability to parse your feelings might be a user's best defense.

www.librarystack.org/go-rando

4. EQUATIONS GROUP TOOLS

In the summer of 2016, a suite of hacking tools appeared for auction from a previously unknown group called "The Shadow Brokers," who claimed to have hacked these tools from another secretive organization, the "Equations Group." A folder of firewall tools was released for free as proof of the hack's overall legitimacy; The Shadow Brokers asked for one million Bitcoin (about 570 million dollars) for the rest of the tools. The free folder featured exploits (components of a larger attack that leveraged security vulnerabilities), implants (covert software developed for targeted attacks on a particular device, usually for surveillance), and tools (general purpose software for active reconnaissance and development), and they ring out with the absurdist naming conventions of the US military: POLARPAWS, EPICBANANA, EXTRABACON. A few of these had been referenced previously in the trove of documents released by Edward Snowden. It is widely presumed that The Shadow Brokers are Russian agents and the Equations Group is a creation of the National Security Agency. And while it is unclear who ultimately bought the full batch of stolen files, the tools were used in massive ransomware attacks in both May and June, 2017, which crippled systems and networks in over 150 countries.

www.librarystack.org/equation-group-firewall-operations

5. NSA REPORT ON RUSSIAN SPEARPHISHING, FALL 2016

Reality Winner, a 25-year-old federal contractor in Georgia who had top-secret clearance, will become the first American charged for leaking documents under the Espionage act during the Trump administration. In

May, Winner anonymously sent an NSA document to *The Intercept* which appeared to prove that Russian state-sponsored hackers had engaged in spearphishing efforts (cyber attacks directed at specific individuals) to disrupt American voting systems, either by duping local precinct officials or the employees of companies who make voting software. The files don't prove these hacks were successful, just that they happened. Subsequent reporting found that these hacking efforts were even more widespread, and targeted voting systems in 39 states. Winner, who served six years in the Air Force as a linguist (she speaks Dari, Pashto, and Farsi), was tracked by the microscopic dot pattern left by her company's color laser printer. Her arrest was announced on June 5th, 2017, just after *The Intercept's* publication of the documents themselves. She is currently awaiting trial.

www.librarystack.org/nsa-voting-hack-dossier-russian-spear-phishing

6. HOUSE RESOLUTION 1125

While hackers wander deep into ostensibly secured systems, millions of refugees are stuck at border camps across the globe. America's reaction to its own immigration crisis has managed to conflate these abstracted paranoias. The first bill proposed by freshman Congressman Jim Banks (Indiana's 3rd) was the Visa Investigation and Social media Act (VISA) of 2017, which would require visa applicants to turn over their social media accounts for vetting by the Department of Homeland Security . Banks tweeted, "This is a common sense way to increase security and ensure those who wish to harm Americans cannot enter the US" even though it's clear enough already that a social media profile will only reveal what a shrewd user wants it to. The bill has been referred to the Subcommittee on Intelligence, where it currently sits.

www.librarystack.org/house-resolution-1125

7. WHITE-COLLAR CRIME PREDICTOR

Sitting somewhere between Minority Report and the Our Revolution PAC, White Collar Crime Risk Zones is a website and app that uses "machine learning to predict where financial crimes will happen across the U.S." The logic of predictive policing has long been applied to "street" level crime (drugs, assault, etc), but has rarely (if ever) been applied

to the financial crimes of mostly white, middle- or upper-class criminals. While turning the technology on the bankers can't help but seem tongue-in-cheek, there's nothing funny about swindling people, nor anything evidently unserious about the software's efforts to map the potentiality of financial crime. The app's system was trained on financial malfeasance reports going back to 1964, and by referencing events with geotagged cartography it can predict where financial crimes will happen at the city-block level with a reported accuracy of 90%. Further, the app uses facial recognition software to give the user a readout of the most likely culprit, should they enter a geographic zone with high statistical potential. Unsurprisingly, it's always a generic white guy. While this *reductio ad absurdum* strategy shrewdly skewers social racism, it also recalls the long history of using photographic imaging to make false predictions and arrests, and points to the (many, obvious) darker uses of AI.

www.librarystack.org/white-collar-crime-risk-zones

8. COMPAS DATA AND ANALYSIS TOOLS

Within the American criminal justice system, the Northpointe corporation's COMPAS algorithm is one of many that are used to determine recidivism rates: the likelihood that a prisoner will commit further crimes and return to prison. After extensive tests and analysis on the prison statistics of a single county in Florida, the journalism foundation ProPublica found that COMPAS disproportionally mis-identitied black prisoners as having higher recidivism likelihoods and white prisoners as having lower ones, thereby affecting sentencing outcomes and treatment by the system. Though Northpointe disputed their results, ProPublica found that the questionnaire used to produce individual datasets for each defendant encodes legacy presumptions about race, class and criminality, despite race itself not being explicitly touched on in the process. Since recidivism stats are used in sentencing guidelines, the program's intrinsic biases continue to have concrete impacts on thousands of defendants — everything from prison term lengths to post-release hiring practices and job placement. Algorithmically-derived quantification and analysis could be used to make the criminal justice system more equitable, distributing more appropriate parole conditions and sentence lengths, but not if the platform has preprogrammed human biases.

www.librarystack.org/compas-data-and-analysis-tools

9. REALEYES WHITEPAPER

Realeyes is a commercial platform that performs real-time measurement of emotional responses to video stimuli through facial recognition AI modeling. Using (with consent, for now) the intake of webcam feeds, the platform records and analyzes the shape of facial responses while a subject watches a video, helping advertisers and marketers learn how to reach a consumer's core sense of decision-making more effectively. Founded at Oxford University in 2007, Realeyes shares some traits with the now-famous Cambridge Analytica company, as it derives actionable (and expensive) data from the aggregated emotional reactions of thousands of users. This stunningly benign-seeming white paper lays out the psychological and neural-network background for the company's commercial services. Triteness may make the cliché, but here the video *is* watching you back, and it is recording every fractional twinge of facial muscle and every squint of the eye, parsing your confusion from your deflation, your enthusiasm from your eagerness. The better it knows you, the better it knows how to make you want things, and the better it helps others to sell them to you.

www.librarystack.org/realeyes-white-paper

*