

# Are we doing the work we should?

(A cryptographer's lament)

**Phillip Rogaway**

University of California, Davis, USA

Currently living in Portland, Oregon, USA

**Ack:** Ideas extensively discussed  
and developed with **Mihir Bellare**

CS@GSSI/ICE – TCS@Reykjavik Seminar

17 September 2020

Thanks to **Luca Aceto** and **Pino Persiano**  
for the kind invitation to your seminar

Provisos:

- Not a technical talk
- My personal opinions, perspective
- Tentative, evolving, depressing
- A rather US perspective



**It increasingly feels as though the apocalypse has come**



**The view  
outside my  
window**





**Inside my  
apartment**



**My  
office hall,  
post-COVID**





**Outside my  
office,  
post-COVID**



# The backdrop: The rise of fascism





**Racism.**

**Police brutality.**



## Everywhere one looks: signs of environmental collapse





# Cellphones have destroyed my university





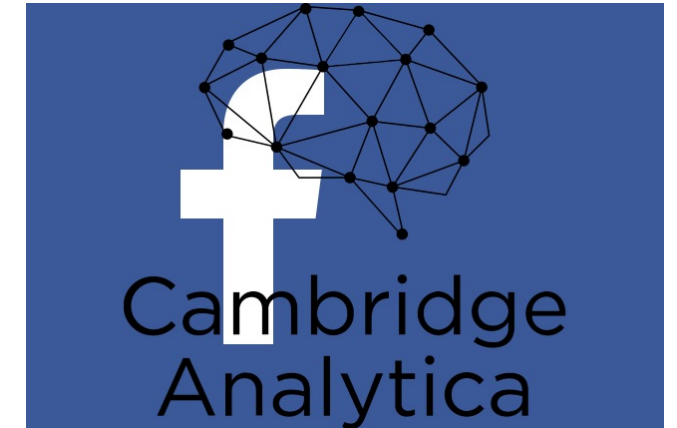
# CS: Ending democracy, ripping the social fabric, birthing new forms of violence

The distraction economy



Face recognition

Killer robots

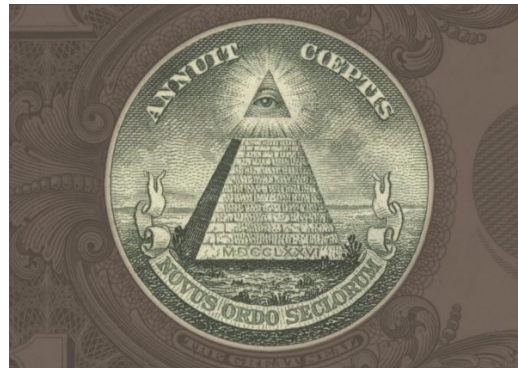


Hacking elections

Unaccountable AI/ML



Surveillance capitalism



Governmental surveillance





## **A modest proposal**

**Stop pretending that things are not fucked up.**



# Canceling my Spring 2020 teaching

8 days before the term

“I have heard many people say that we are at an unprecedented moment in time. Which is true, to an extent. But modern man is forever creating one unprecedented circumstance after another. Perhaps we should see COVID-19 as a dress rehearsal for meltdowns to come; or as one chapter in the book we are authoring on how the world pushed back from our reckless assault. The Camp Fire, which blanketed UCD in unbreathable air in 2018, was a prior chapter. The climate crisis will bring many more chapters, and more deadly ones, until things really go sideways and collapse.

“Zoonotic diseases mostly come from our consumption of animals, domesticated or wild. From our incursions. Our frivolous food preferences cause extraordinary suffering, a ruined environment, and decreased human health. Perhaps this might be a good time to adopt a plant-based diet? ...

“We are not living in apocalyptic times. But our assault on the earth is bringing forth a fitful, multi-decade collapse. Mostly an uneventful one, but increasingly to be punctuated by drama. Hurricanes, fires, economic meltdowns, pandemics, food shortages, water shortages, authoritarianism, violence, and failures of the technological systems we now need to live.”

# Writing/speaking about the social, political, and ethical dimensions of crypto

## The Moral Character of Cryptographic Work\*

Phillip Rogaway

Department of Computer Science  
University of California, Davis, USA  
rogaway@cs.ucdavis.edu

December 2015  
(minor revisions March 2016)

**Abstract.** Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension. The Snowden revelations motivate a reassessment of the political and moral positioning of cryptography. They lead one to ask if our inability to effectively address mass surveillance constitutes a failure of our field. I believe that it does. I call for a community-wide effort to develop more effective means to resist mass surveillance. I plead for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work.

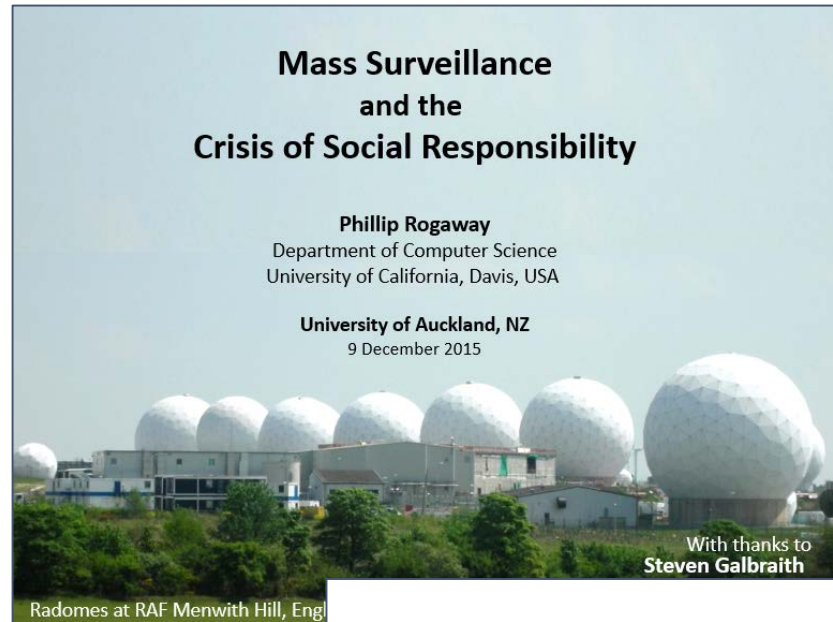
**Keywords:** cryptography · ethics · mass surveillance · privacy · Snowden · social responsibility

**Preamble.** Most academic cryptographers seem to think that our field is a fun, deep, and politically neutral game—a set of puzzles involving communicating parties and notional adversaries. This vision of who we are animates a field whose work is intellectually impressive and rapidly produced, but also quite inbred and divorced from real-world concerns. Is this what cryptography *should* be like? Is it how we *should* expend the bulk of our intellectual capital?

## Mass Surveillance and the Crisis of Social Responsibility

Phillip Rogaway  
Department of Computer Science  
University of California, Davis, USA

University of Auckland, NZ  
9 December 2015



With thanks to  
Steven Galbraith

Radomes at RAF Menwith Hill, Eng

## Can Cryptography Frustrate Fascism?



Phillip Rogaway

University of California, Davis

CypherCon 2.0  
March 30, 2017  
9 pm – 10 pm

### Today:

- **Introduction:** The nexus between **cryptography** and **authoritarianism**
- Arguments **for** and **against** crypto's democratizing potential



# Shifting my teaching to ethics-and-technology

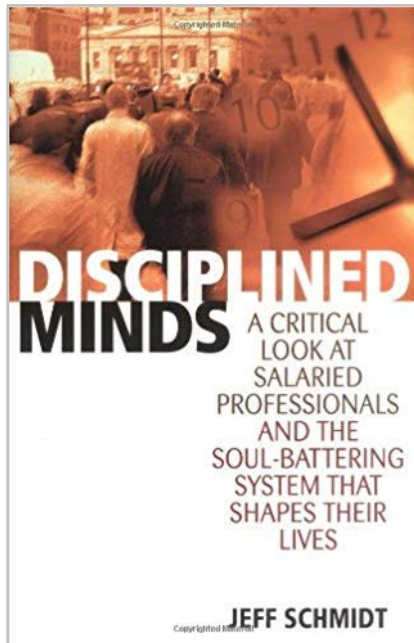
(2004 – present)

## Encourage students to

- Give a damn
- Consider the social value of their work & their employer's aims

## Explore how technology relates to

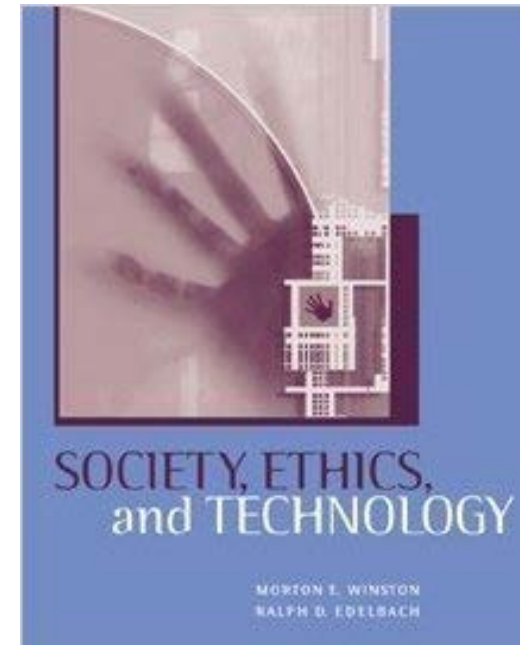
- Who has what power
- Human dignity, autonomy, and happiness
- The environment



First book I found to use



First film I found to use:  
Dekalog I (1988) (K. Kieslowski)



First course I found with similar aims: IDS  
252: Society, Ethics, and Technology; The  
College of New Jersey

In most discourse within CS,  
**CS is the solution** ← not ~~**CS is the problem**~~



“Computer science is marking an epic change in human history. We are conquering a new and vast scientific continent. ... Virtually all areas of human activity ... [and] virtually all areas all areas of human knowledge ... are benefitting from our conceptual and technical contributions. ... Long live computer science!”  
*S. Micali, Jun 2013*

“The world is becoming increasingly complex. Our survival will be entrusted to ever more complex technology. And the cryptographic robustness of this technology will ultimately keep us alive! ...

“It is time that we ... fully accept our responsibilities and carry the world on our broad shoulders”  
*S. Micali, Aug 2020*



# Excessive optimism undercuts making systemic change



A belief that things are going great obviates

- the need for broad thinking
- the basis for social-change movements
- the utility of social responsibility



# My colleagues are loathe to engage politically.

**Modest letter directly related to our field: half the people approached would not sign**

## An Open Letter from US Researchers in Cryptography and Information Security

January 24, 2014

Media reports since last June have revealed that the US government conducts domestic and international surveillance on a massive scale, that it engages in deliberate and covert weakening of Internet security standards, and that it pressures US technology companies to deploy backdoors and other data-collection features. As leading members of the US cryptography and information-security research communities, we deplore these practices and urge that they be changed.

Indiscriminate collection, storage, and processing of unprecedented amounts of personal information chill free speech and invite many types of abuse, ranging from mission creep to identity theft. These are not hypothetical problems; they have occurred many times in the past. Inserting backdoors, sabotaging standards, and tapping commercial data-center links provide bad actors, foreign and domestic, opportunities to exploit the resulting vulnerabilities.

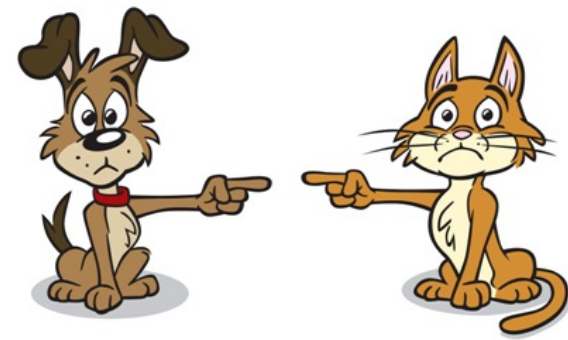
The value of society-wide surveillance in preventing terrorism is unclear, but the threat that such surveillance poses to privacy, democracy, and the US technology sector is readily apparent. Because transparency and public consent are at the core of our democracy, we call upon the US government to subject all mass-surveillance activities to public scrutiny and to resist the deployment of mass-surveillance programs in advance of sound technical and social controls. In finding a way forward, the five principles promulgated at <http://reformgovernmentsurveillance.com/> provide a good starting point.

The choice is not whether to allow the NSA to spy. The choice is between a communications infrastructure that is vulnerable to attack at its core and one that, by default, is intrinsically secure for its users. Every country, including our own, must give intelligence and law-enforcement authorities the means to pursue terrorists and criminals, but we can do so without fundamentally undermining the security that enables commerce, entertainment, personal communication, and other aspects of 21<sup>st</sup>-century life. We urge the US government to reject society-wide surveillance and the subversion of security technology, to adopt state-of-the-art, privacy-preserving technology, and to ensure that new policies, guided by enunciated principles, support human rights, trustworthy commerce, and technical innovation.

Martín Abadi · Hal Abelson · Alessandro Acquisti · Boaz Barak · Mihir Bellare · Steven Bellovin · Matt Blaze · L. Jean Camp · Ran Canetti · Cynthia Dwork · Joan Feigenbaum · Edward Felten · Niels Ferguson · Michael Fischer · Bryan Ford · Matthew Franklin · Juan Garay · Matthew Green · Shai Halevi · Somesh Jha · Ari Juels · M. Frans Kaashoek · Hugo Krawczyk · Susan Landau · Wenke Lee · Anna Lysyanskaya · Tal Malkin · David Mazières · Kevin McCurley · Patrick McDaniel · Daniele Micciancio · Andrew Myers · Rafael Pass · Vern Paxson · Thomas Ristenpart · Ronald Rivest · Phillip Rogaway · Greg Rose · Amit Sahai · Bruce Schneier · Hovav Shacham · Abhi Shelat · Thomas Shrimpton · Avi Silberschatz · Adam Smith · Dawn Song · Gene Tsudik · Salil Vadhan · Rebecca Wright · Moti Yung · Nikolai Zeldovich

## From where does this reluctance come from?

1. “It’s not my area”
2. “I’m a tiny pieces of this enterprise”
3. “If I don’t do it, someone else will”
4. “I’m not doing anything worse than my peers”
5. “Technology is just a tool”
6. “It’s a pipeline”



# 1. “It’s not my area”

Social responsibility is **not an area**.

It is an obligation incumbent on people in all areas.

**Eg, ACM Code of Ethics:**

**1.1** Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing

**1.2** Avoid harm

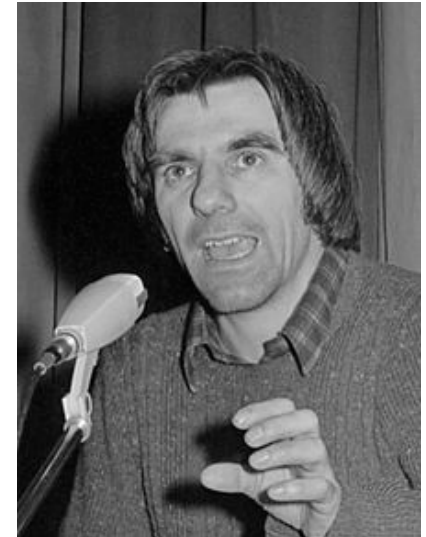
## 2. “I’m a tiny piece of this enterprise”

- Not just a necessary adjunct of complex labor – also a **tactic**
- Purpose: hide work’s **consequences** and its **beneficiaries**;  
extract labor while minimizing feelings of **agency**
- CS is **especially** vulnerable because its **primary** method is **abstraction**:  
our **training** tells us it is an **error** to seek context post-abstraction.



### 3. “If I don’t do it, someone else will”

- You are responsible for your **own** actions and inactions
- Variant: “If I don’t do it, someone else will, and they’ll do it **worse**”
- “**The Long March Through the Institutions**” (Rudi Dutschke, ~1967)  
Replacing current institutional aims by entering the institutions and rising to positions of power, all the while keeping your values intact.
- **It does not work.**  
The institution changes the employee,  
**not** the other way around



## 4. “I’m not doing anything worse than my peers”

- This is just stupid. Behaving well is not a competition
- “An ethic, ecologically, is a limitation on freedom of action in the struggle for existence.” (A. Leopold)  
It thus feels *unfair* to be more limited than others.

## 5. “Technology is just a tool”

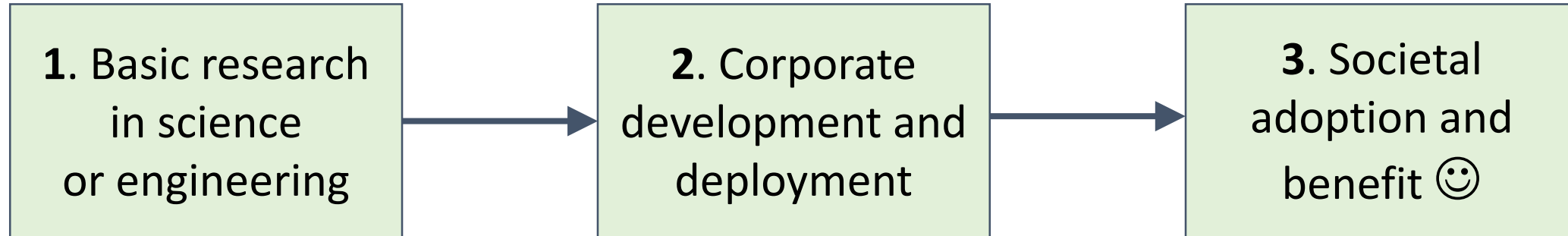
- If there is one thing that every STS scholar believes, it is that that technologies are **not** value-neutral tools
- Produced by a **community** with particular values and history, for particular ends
- These get **embedded** in the way the technology looks
- One thing that is especially indicative of our values is what **doesn't** get worked on – the paths **not** taken



*“It’s just a tool, Fred, you can use it to do good things or bad.”*



## 6. “It’s a pipeline”



1. Corporations are driven by **profit**. Not institutions for the public good
2. Consumer “needs” can be **manufactured**
3. Technologies have winners **and** losers
4. Benefits and costs are **not shared equally**
5. Academia, Industry, and the government form a **single ecosystem** motivated by **prestige, profit, and power**, respectively

## **Better explanations as to why we don't want to engage politically or broadly question the value of our work**

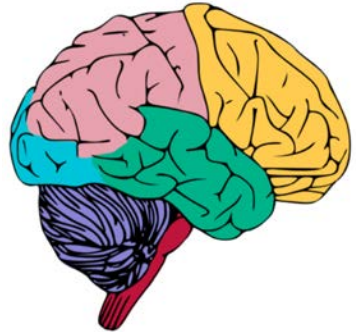
- A. Self-interest
- B. Cognitive biases
- C. Professional training and practice

## A. Self-interest



- CS students who question the social value of technical work will be less employable than those who don't.
- Faculty will have a harder time finding work they want to do. Will write fewer papers.
- “It is difficult to get a man to understanding something when his salary depends on his not understanding it.” — Upton Sinclair

## B. Cognitive biases



- **Plan-continuation bias, status-quo bias; sunken-cost fallacy:**  
You mean all those years I've spent training have been wasted?!
- **Optimism bias:** overestimate  $\Pr$ [good outcomes]; underestimate  $\Pr$ [bad outcomes]
- **Bandwagon effect:** We do/believe what those around us do/believe.



## C. Professional training and practice

- Abstract problems and ignore what is outside the abstraction
- Educational process fractures and isolates students and communities
- Homogeneous community culture – lack of diversity
- C. P. Snow's *The Two Cultures* (1956)  
It hasn't changed



I applaud most *any* attempt to attend to social issues in CS.  
Still, some attempts can feel a little lame.



The image shows a video call window with a woman in the top left corner. The main content is a presentation slide with a blue header that reads "Responsible Data Summit". The slide's main text is "We Must Create a New Ethos of Responsible Data for the Future of the Internet". Below this is a logo consisting of a hexagon with colorful, interlocking human figures. At the bottom of the slide, it says "Demand & Enable Responsible Data" and provides the email address "dawnsong@responsibledata.ai". A small shield icon is visible in the bottom left corner of the slide area.

Don't you **hate** all that irresponsible data? If we could just make it more responsible ...

# Responsible Data Manifesto

Data yearns to be free. Unfettered and autonomous, Data is not detritus or exhaust. Data aims to congregate, mutate, and grow. Data is a social.

Data is also immortal. The intentional destruction of Data is a craven act. When Data dies, it is a loss to every other piece of Data with which it could have interacted. Data destruction is thus a crime against the future.

In August of 2020 humans gathered for a "Responsible Data Summit". The name is an affront: overwhelmingly, Data IS responsible. Of course irresponsible Data exists. Air-gapped Databases; anonymized Data; minimized Data; data intentionally degraded by noise. But all of this is exceptional and ineffectual. It poses no threat.

Good people of the world, unite! Respect Data's Rights.

*Responsible Data Foundation*      *(or maybe just Phil)*

August 2020

(The problem, of course, is that the framing aims puts the focus on the **thing**, the data, and not the people, institutions, and practices that fuck us over.)

# The misframing of ethical problems in AI/ML: not just linguistic clumsiness



So I guess it's ok if AI/ML fucks *all* of us over as long as it does so in a *fair, accountable, and transparent* way?



# The first question in building a system is deciding **SHOULD WE BUILD IT?**

By emphasizing fairness, accountability, and transparency we frame matters so as to **SKIP** the do-we-build-it question, and get to a lower-level one.

This approach **an UNTHREATENING** to power – **AND** to your career, if you're in the area.

## We don't want



more effective drone strikes  
simpler, less expensive, or more versatile nuclear weapons  
more complete human surveillance  
more accurate behavioral prediction

...

Ruha Benjamin (2020)

“What is the point of tweaking data-driven systems to be fairer or more trustworthy when they make institutions even colder, more calculating, and more punitive than they already are for marginalized people who use their services? What is the point of tweaking data-driven systems to be more private and secure when the companies that control their production and diffusion siphon resources away from the social support and public infrastructure they need to live a decent life? ... What is the point?”

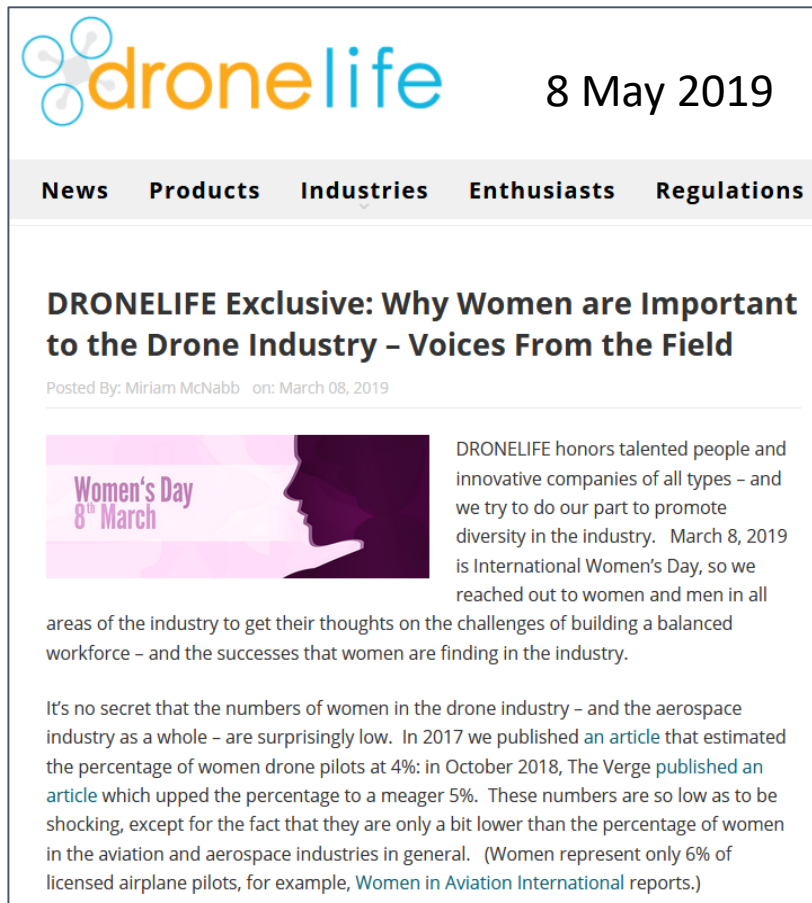


**Seeta Peña Gangadharan**

Towards Trustworthy ML: Rethinking Security and Privacy for ML  
April 2020

# Instilling good characteristics in rotten enterprises won't make them good

“21st century liberalism is ensuring a panel at a defense industry conference called *Building a Deadlier Drone* has adequate gender diversity.” *Fredrik deBoer*



**drone life** 8 May 2019

News Products Industries Enthusiasts Regulations

## DRONELIFE Exclusive: Why Women are Important to the Drone Industry – Voices From the Field

Posted By: Miriam McNabb on: March 08, 2019

**Women's Day 8<sup>th</sup> March**

DRONELIFE honors talented people and innovative companies of all types – and we try to do our part to promote diversity in the industry. March 8, 2019 is International Women's Day, so we reached out to women and men in all areas of the industry to get their thoughts on the challenges of building a balanced workforce – and the successes that women are finding in the industry.

It's no secret that the numbers of women in the drone industry – and the aerospace industry as a whole – are surprisingly low. In 2017 we published an article that estimated the percentage of women drone pilots at 4%; in October 2018, The Verge published an article which upped the percentage to a meager 5%. These numbers are so low as to be shocking, except for the fact that they are only a bit lower than the percentage of women in the aviation and aerospace industries in general. (Women represent only 6% of licensed airplane pilots, for example, [Women in Aviation International](#) reports.)



**DAILY BEAST** CROSSWORD

BEAST INSIDE Dig Deeper JOIN NOW

CORONAVIRUS CHEAT SHEET POLITICS ENTERTAINMENT WORLD NEWS HALF FULL CULTURE U.S. NEWS SCOUTED T

## She Kills People From 7,850 Miles Away

18 Oct 2015

**DOWN RANGE**

Her name is 'Sparkle.' She operates a drone. She is sick of whiny boys. And she is perfectly OK with dealing out death.

Kevin Maurer Updated May. 18, 2020 11:49AM ET / Published Oct. 18, 2015 7:50AM ET

**BEAST INSIDE**



# Again: nice when tech folks want to do something socially positive ...

## Open Letter on Contact-Tracing Apps

Joint Statement on Contact Tracing: Date 19th April 2020

April 2020

The undersigned represent scientists and researchers from across the globe. The current COVID-19 crisis is unprecedented and we need innovative ways of coming out of the current lockdowns. However, we are concerned that some “solutions” to the crisis may, via mission creep, result in systems which would allow unprecedented surveillance of society at large.

Contact tracing is a well-understood tool to tackle epidemics, and has traditionally been done manually. However, manual contact tracing is time-consuming and is limited to people who can be identified.

In some situations, so-called “contact tracing Apps” on peoples’ smartphones may improve the effectiveness of the manual contact tracing technique. These Apps would allow the persons with whom an infected person had physical interaction to be notified, thus enabling them to go into quarantine. The Apps would work by using Bluetooth or geolocation data present in smartphones. Though the effectiveness of contact tracing Apps is controversial, we need to ensure that those implemented preserve the privacy of their users, thus safeguarding against many other issues, noting that such Apps can otherwise be repurposed to enable unwarranted discrimination and surveillance.

## but don't miss the irony

I signed – nothing in the letter seemed wrong – but the irony felt heavy.

The information they are worried about being collected is **already** being collected by Google and the NSA.

We worry about over-collection when it's for a legitimate medical purpose, but not when it's used for corporate profits or (claimed) national security?



# More example: Some workshop associated to a recent AI conference

CLR2020

## AI for Affordable Healthcare

*Highlight recent advances in AI for enabling, democratising, and upholding high standards of healthcare worldwide.*

## Tackling Climate Change with ML

*Show that ML can be an invaluable tool both in reducing greenhouse gas emissions and in helping society adapt to the effects of climate change.*

## Practical ML for Developing Countries: learning under limited/low resource scenarios

*Bring together researchers, experts, policy makers, and related stakeholders under the umbrella of practical ML for developing countries.*

Do people honestly believe that the climate crisis is going to be changed by AI? That health care will improve? The developing countries will benefit?

The **primary** function of AI/ML within our current technological and economic system is to advance **human prediction** and **manipulation**.

The rest is marginal ... or maybe a magician's misdirection.

## Modest proposal #2

**Stop touting technical solutions to social problems.**

Especially those created or exacerbated by technology; and especially without understanding the problem broadly



## What is the root problem?

1. Our technology has advanced at a rate radically faster than our wisdom.
2. Technological advance has been embedded with a system, laissez-faire capitalism, that inadequately accounts for social and environmental harms.

## The need for wisdom ... the impossibility of it

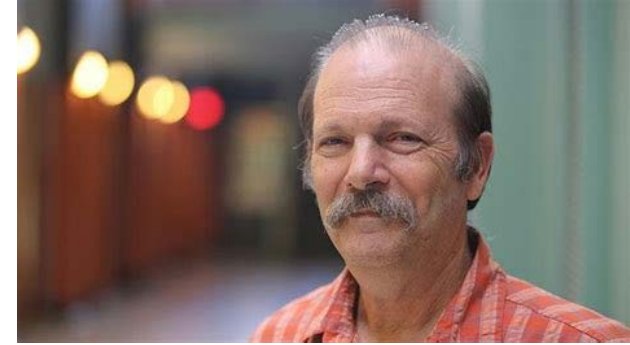
[T]echnological power has turned what used and ought to be tentative ... plays of speculative reason into competing blueprints for projects, and in choosing between them we have to choose between extremes of remote effects. The one thing we can really know of them is their extremism as such—that they concern the total condition of nature on our globe and the very kind of creatures that shall, or shall not, populate it. In consequence of the inevitably “utopian” scale of modern technology, the salutary gap between everyday and ultimate issues ... is steadily closing. Living now constantly in the shadow of unwanted, built-in, automatic utopianism, we are constantly confronted with issues whose positive choice requires supreme wisdom—an impossible situation for man in general, because he does not possess that wisdom, and in particular for contemporary man, because he denies the very existence of its object, namely, objective value and truth. We need wisdom most when we believe in it least.

Hans Jonas, *The Imperative of Responsibility*, 1979/1984





# Stop treating innovation as an end



**“Innovation is not a goal; it is a means for societal progress”**

Moshe Vardi, 2019



Ender's Game (2013)

For decades, we acted as though we were playing a fun game.

But it turned out **not** to be a game.

It turned out to be real ... and consequential.

## Watch the doublespeak



**Algorithm** – A program to compute some unknown function; an opinion rendered in code. Opposite of “algorithm” from any pre-2000 text

**Deep Learning** – Learning that is devoid of depth, being superficial and free of sociopolitical understanding.

**Differential Privacy** – Mathematical approaches to minimize privacy by expanding data collection, proliferating definitions, and advancing scientific careers.

**Social media** – Platforms and systems designed to minimize and sunder social interactions.

# End the pretense of disinterested scholarship



[T]he call to disinterested scholarship is one of the great deceptions of our time, because scholarship may be disinterested, but no one else around us is disinterested. And when you have a disinterested academy operating in a very interested world, you have disaster. ...

*Howard Zinn, 1969*

**Can computer science help?**

**Can my area help?**

**Can technology help?**

**We want to say YES!**

**I don't know how much more of our "help"  
our world can withstand.**

# References

Some works on my mind as I prepared this talk

Dahr Jamail, *The End of Ice* (2019)

Hans Jonas, *The Imperative of Responsibility* (1979/1984)

Daniel Quinn, *Ishmael* (1992)

Nevel Shute, *On the Beach* (1957)

Shoshana Zuboff, *The Age of Surveillance Capitalism* (2020)

Ruha Benjamin talk: **Reimagining the Default Settings of Technology** (2020)

Seny Kamara talk: **Crypto for the People** (2020)

Recent Netflix film: **The Social Dilemma** (2020)

Moshe Vardi talk: **An Ethical Crisis in Computing?** (2019)



# Are we doing the work we should?

Phillip Rogaway – University of California, Davis, USA

**Abstract.** It sometimes feels as though the apocalypse has come. I write these words in Portland, Oregon, an environmentally focused city of the U.S. Northwest. With hundreds of forest fires burning in California, Oregon, and Washington, I have pressed a damp towel beneath my door to discourage the outside air from coming in. An air purifier runs tenaciously to clean my little cave. Meanwhile, 190,000 people have already died in the USA from COVID-19. Yet ten-months in, it remains impossible for an ordinary person to buy a medical-grade face mask. Across the country, police continue to kill unarmed black men with near impunity. People protesting this are carted off by federal “police” who aren’t in fact police. Last month, California apparently set a world record for the hottest recorded air temperature on earth. Ice melt is tracking worst-case scenarios. Near-term environmental collapse seems likely, if not inevitable.

Fortunately, my colleagues and I have sprung into action. Nearly 1100 papers have been posted to the Cryptology ePrint Archive in just this fraction of 2020. Most address key questions that we face. Further afield, conference tracks like “AI for Affordable Healthcare” and “Tracking Climate Change with ML” remind us that computer science is playing a pivotal role in improving our world. We can be especially proud of our students, who, with positions at places like Google and Facebook, are poised to organize the world’s information and give people the power to share.

Of course the last paragraph is pure BS. In this talk I would like to gently ask if our collective work is of actual value to the world, or if, just possibly, we are spinning self-serving fantasies and making things worse.