For too long, technology companies have lobbied their friends in Congress to avoid meaningful regulation and oversight. The companies have claimed that "self regulation" is the best way to ensure they meet their legal and ethical obligations. But time and time again, the companies have failed -- whether it's keeping human trafficking off their sites, addressing the rise of bullying and hate speech on their platforms, or preventing foreign governments from interfering in our elections. Congress has also neglected its responsibility to ensure that the benefits of technology and the digital economy reach all Americans, not just company executives and investors.

Ross LaJeunesse knows that with the right government oversight, we can ensure that all Mainers and Americans benefit from the widespread use of technology. From his years of government service, his experience at Google, and from teaching technology policy at both Georgetown and George Washington Universities, he's developed an expertise in technology and technology policy that he'll use to bring new investment, businesses and jobs to Maine. He will also ensure vigilant Congressional oversight over technology companies, and introduce much-needed legislation to address critical areas where technology companies and our federal government have let us down.

1. HIGH SPEED INTERNET FOR ALL

High speed internet is the infrastructure of the future and must be available to all Americans at affordable rates, including those living in rural areas. Access to high speed internet will determine the future economic and societal health of Mainers.

The Problem:
Too many Mainers, especially those living in rural areas, don't have access to affordable, high-speed internet. These areas of our state will fall further and further behind economically, culturally, and in educating our children. Ross wrote one of the first comprehensive plans in the nation to increase internet coverage when he worked in California in 2005. Today California ranks 13th in the country in high speed internet access, despite its vast rural areas, while Maine ranks 45th.¹

Ross’s Solution:
Maine needs to aggressively seek its fair share of the $9 billion fund just announced by the Federal Communication Commission to bring high-speed internet to rural areas.² But, even that federal funding is not enough to wire Maine for the future. We must use federal and state funding to deploy high-speed internet with the same determination and focus we used to

connect rural areas with electricity in the 1930s. High-speed internet is a basic right, and no Mainer should be left behind.

Finally, the federal government must study whether internet access should be regulated as a utility, with appropriate consumer protections and price controls.

2. PRIORITIZE AMERICAN WORKERS
Technology can be a significant source of new job creation and opportunity when the right government policies are in place, and when corporations are held accountable for doing the right thing, instead of only caring about profits.

The Problem:
Our economy is facing a tidal wave of job losses from the increasing use of automation and artificial intelligence (AI). Yet, too few people in Washington seem to know or care about this critical issue. The workers most likely to be impacted by automation are those already most vulnerable economically: cashiers, retail employees, drivers, and assembly line workers. Globally, it's projected that 20 million manufacturing jobs will be lost in the next ten years due to automation.³

Ross's Solution:
The federal government must develop a comprehensive strategy for addressing the changes in our economy and especially the impact on our workers by partnering with technology companies, industries most likely to be impacted, unions, economists, and other experts -- and it must commit the necessary federal funding to ensure every displaced worker is given no-cost job re-training, skills development, and temporary financial assistance while they transition into new jobs. Just as important, as all companies continue to incorporate more technology into their business operations, they must provide appropriate training and tuition assistance for re-/ up-skilling programs to enable workers to transition to new jobs.⁴

There is already high demand for skilled laborers and tradespeople. Our economy will need over 60,000 new electricians in the next six years.⁵ Bath Iron Works is currently seeking 1,000 skilled workers in order to bid for a multi-billion dollar Coast Guard contract.⁶ Maine and the rest of the country are also in desperate need of new infrastructure, which could create 16 million

⁴ https://www.brookings.edu/blog/the-avenue/2019/02/25/automation-and-ai-will-disrupt-the-american-labor-force-heres-how-we-can-protect-workers/
⁵ https://www.foxbusiness.com/economy/electrician-shortage-six-figure-salary-job
new construction jobs. In Maine alone, our bridges need $50 billion in repairs. We must prioritize helping displaced workers find new and better-paying jobs that will not only give them and their families a better life, but also meet the current and future needs of Maine, our country, and our economy.

3. SECURE AMERICANS’ PRIVACY

Americans generate a tremendous amount of data about themselves and their activities every day while on their computers, phones, and other devices. Over 90% of all the data in the world was produced in just the past two years.

The Problem:
The data of individuals is used, stored, and often sold by the internet, technology and communications companies that collect it -- usually without the individual knowing or agreeing to this. These companies make massive profits using this data, and are not transparent about what data is collected or how it is used, including when that data is sold. This is not acceptable.

Since the federal government has failed to protect Americans, various states have passed legislation to protect privacy, but these laws are confusing and often differ from one state to another. For example, Maine has a consumer privacy law but it only applies to internet service providers (ISPs) and does not regulate large technology companies like Apple, Facebook, Amazon, and Google.

Ross’s Solution:
Congress must pass comprehensive privacy legislation that makes it clear that individuals:

- own their own data,
- have the right to full transparency about what user data a company collects and how it uses that data,
- have the right to decide if and how their own data is collected and used, and
- cannot be denied the use of a company’s services solely due to their refusal to allow the company to collect and use their data.

---

Finally, if a company earns income from selling an individual's data, that person -- as the owner of that data -- should be entitled to share in the profits made through its sale (a "data dividend").

4. PROMOTE DIGITAL EDUCATION and DIGITAL CITIZENSHIP
Our children are very skilled at using mobile devices and applications, especially social media. However, too many of them don't have the skills needed to fully participate in the economy of the future, or to even ensure they remain safe online.

The Problem:
The internet, mobile devices, and applications are central to the lives of most teenagers and even younger children. In fact, a recent study found that teens spend an average of 7 hours and 22 minutes per day watching videos, playing video games, and using social media -- and this does not include time using a computer for school or homework. Yet, we are not teaching them the skills and giving them the tools they need to stay safe online, or how to be "digital citizens." In the absence of federal leadership, non-profit organizations such as Common Sense Media have worked hard to address this urgent need. States such as Wyoming are requiring students to take computer science courses. Other countries, such as France, have programs that teach students how to detect fake news online, check the sources of online information, and stop online bullying.

Ross’s Solution:
The United States must prioritize teaching all our students computer science and digital skills, and also prepare them to be digital citizens. This will help our students stay safe from online bullies and predators, prepare them to participate as innovators and entrepreneurs in an economy where technology is central to every business, and also arm them with the skills needed to ensure that the internet and technology platforms work toward the advancement of freedom, knowledge and human rights -- rather than the opposite. Working in partnership with civil society, technologists, technology companies, education experts and others, the federal Department of Education should move swiftly to develop model curricula, develop training modules for teachers and counselors, and then must provide sufficient funding for states to implement these programs as soon as possible.

5. DEFEND AGAINST CYBERATTACKS and ELECTIONS INTERFERENCE

11 https://www.commonsense.org/
The United States has a well-trained and well-funded military, but we are not adequately prepared for the most likely threat to our country, economy, infrastructure, and democracy: cyberattacks.

The Problem:
We are under constant threat of cyberattacks. Last year, more than 70 local and state government agencies paid ransom to hackers who disabled computer systems and databases. Corporations also play a role in these problems by failing to keep their infrastructure, products, and customers' data safe. Last year alone, over 10 billion data records were breached. In addition, foreign actors tried to influence our 2016 election by placing false political ads and using "bots" on online platforms. Still, Facebook recently announced that it will not monitor political advertising for accuracy, effectively putting profits ahead of truth and our democracy.

Ross’s Solution:
The United States must develop and fully fund a comprehensive national strategy to ensure the security of our citizens, economy, critical infrastructure, and our elections. Corporations also must be held responsible for breaches to their networks and attacks that threaten our democracy, through increased fines and other penalties. We also need to ensure our voter data and voting machines are secure and able to withstand cyberattacks and sophisticated hacking attempts. Sufficient federal funding must be provided to the states for the purchase of best-in-class voting machines with paper receipts and other critical election infrastructure, along with adequate training for all election officials.

Finally, political ads online should be subject to the same regulations as political ads on television and radio.

6. PROTECT CONSUMERS and THE FREE MARKET
The role of technology in our lives and our economy continues to advance at a break-neck pace, posing challenges to consumers and our free market economy.

The Problem:
The growing economic and societal power of technology companies and platforms requires greater government review and oversight. It is important that the federal government -- through the Federal Trade Commission (FTC) and the Department of Justice -- closely examines

---

technology companies’ influence on the American economy to ensure that consumers are benefiting from free and fair competition.

Ross’s Solution:
The FTC currently conducts anti-trust reviews of consumer harm using the “consumer welfare” model, with a focus on financial harm. It is imperative that we reevaluate this focus as companies and business models continue to evolve and raise new challenges beyond economic costs to consumers. Issues like the market dominance of technology platforms and the amount of user data they have, and the impact this has on consumers' privacy, autonomy, and agency must be considered -- elements that are critical to a truly competitive marketplace.

7. ADVANCE CIVIL and HUMAN RIGHTS
One of the most critically important roles of our government is to protect and promote the civil rights and the human rights of every individual. This responsibility can not be ignored, nor left in the hands of corporations or any other institutions, regardless of how convincing their public relations and marketing plans might seem.

The Problem:
Technology is increasingly central to our daily lives and activities. As a result, we must focus on ensuring that the technologies, applications, and platforms Americans use every day -- as well as the companies that own and develop them -- uphold and promote civil and human rights. Yet, too often technology companies have shown a willingness to put profits ahead of principles and doing the right thing.

Ross’s Solution:
We should enact legislation requiring every company with over $5 million in revenue to designate an officer responsible for civil and human rights compliance. This officer will review the company’s business and product activities and provide an annual report to the U.S. Department of Justice on the company's compliance with existing civil rights laws as well as the Universal Declaration of Human Rights. The Department of Justice should make these reports available online for public review. Federal legislation must provide the funding and staff necessary for the Department of Justice to review the reports and audit company compliance. Federal legislation must also provide appropriate enforcement mechanisms and penalties, including personal liability for company executives deemed responsible for civil and human rights violations.

While whistleblower protections exist for employees in some industries, including for many federal employees, the mix of federal and state laws providing protections to employees in the business sector are often difficult to interpret and vary from state to state. Given the amount of user data held by technology companies and the critical role technology platforms have in our
economy and in every facet of our society, the federal government should pass comprehensive legislation that clarifies and guarantees whistleblower protections for employees of technology companies who disclose corporate behavior that is illegal and unethical, or threatens the rights, safety, or security of users. These protections should cover employees who bring data breaches and security bugs in a company’s technical infrastructure to company management, only to have the company ignore their concerns. A specific "technology whistleblower unit" should be established at the Federal Trade Commission to review employee complaints and pursue appropriate remedies.

8. PROTECT AMERICA’S CRITICAL TECHNOLOGY and INFRASTRUCTURE
America has long been the world's leader in innovation. The ground-breaking work at the University of Maine's Advanced Composites Lab in Orono is a great example of how American ingenuity and creativity will continue to change and improve the world. There are few challenges that Americans can't meet and few problems that American ingenuity and innovation can't solve.

The Problem:
America’s leadership in innovation means that some foreign companies and governments actively seek to steal technologies developed and owned by American businesses and academic institutions. These foreign actors steal our technology and inventions through outright theft, spying, and hacking. In addition, we must be concerned about American companies selling their technology to businesses and governments without regard to the possible impacts on U.S. national security interests and on human rights.

Ross’s Solution:
Our intelligence and law enforcement agencies must partner closely with American companies and institutions that could be targeted to ensure that their innovations are not stolen, and make absolutely certain that any technology that could be weaponized, or used for surveillance, election interference, criminal activities, or other human rights violations will never fall into the hands of malicious actors, including governments hostile to U.S. interests. We must pay particular attention to artificial intelligence and facial recognition technology, as current federal policy has established few limits on how these tools are used, including their sale and export outside the United States.17

Finally, we must review existing regulations on foreign investment in our businesses and domestic infrastructure to ensure that these regulations are keeping pace with both technological developments and shifts in global alliances. Companies and governments with

---

17 https://www.cfr.org/blog/we-need-drastic-rethink-export-controls-ai
interests hostile to the United States should not be permitted to make significant investments in, or gain control over, any critical technology or infrastructure.

9. PREVENT ABUSE OF AI, FACIAL RECOGNITION and DEEPFAKES

Artificial intelligence (AI) is the ability of computer systems to perform tasks and make decisions that have previously required human intelligence and reasoning. Examples include voice-powered digital assistants like Siri, and self-driving vehicles. One form of AI that is quickly being developed and used by businesses and governments is facial recognition technology, which attempts to identify individuals by scanning and analyzing their facial features and then comparing them to known images in a large database.

The Problem:
While AI and facial recognition may provide some benefits to law enforcement, transportation, and security agencies, there are considerable privacy and other concerns with the way the technology is being developed and deployed. For example, Asian and African American faces are 100 times more likely to be mis-identified by even the most advanced technologies.18 Recent reports about the company Clearview AI have highlighted the threat to privacy and other civil rights posed by businesses developing facial recognition services, as it has used photos taken from social media sites to assemble a database of three billion images, and is selling its facial recognition services to 600 law enforcement agencies.19 While some city police forces are currently using facial recognition, other cities have adopted bans on facial recognition technology. In Maine, the State Police have refused to disclose how they’re using advanced technologies, depriving citizens and the media of basic transparency and oversight.20

Deepfakes are AI-produced hyper-realistic video and audio recordings of people appearing to do or say things they actually didn’t. As AI expands, there are now tools that people with little to no technical expertise can use to create deepfakes. This could give anyone the ability to make a fake, but extremely convincing, video for political or other dangerous purposes. At a minimum, the increasing use of deepfakes impacts our ability to trust any audio or video recording as factual, since we won’t be able to detect whether the recording or broadcast we’re seeing and hearing is truly real.

Ross’s Solution:

The opportunities for abuse of these technologies are significant, and decisions about when and how they are used cannot be left to private companies. The federal government must recognize its responsibility to protect the privacy and other civil rights of citizens.

Similar to the approach we must take with user data, we must pass federal legislation that requires greater transparency when facial scans are taken, clarifies that any facial scans taken are owned and controlled by the individual and not the company taking the scan, and require all entities to obtain clear, informed opt-in consent from individuals before the facial scan is stored and used for any commercial purposes.

Congress should move swiftly to regulate deepfakes in a thoughtful and effective way. At the very least, we must prohibit the use of deepfakes in political advertising. More broadly, some proposals have called for clear labeling of all deepfakes, but we must be sure that we are able to effectively enforce such labeling requirements. Congress should appoint a bipartisan expert commission on AI, comprised of civil society, academia, business, and government experts to explore and define the appropriate limits of facial recognition, biometric technologies, deepfake technology, and other artificial intelligence. The commission should address clear ethical principles for these technologies, and provide recommendations to Congress on legislation and regulation needed to protect individual civil and human rights, including proper oversight of local, state, and federal government use.

10. GUARANTEE A FAIR MARKET THROUGH NET and PLATFORM NEUTRALITY

"Net neutrality" is the principle that internet providers must treat all communications on their networks equally and not intentionally block or slow down some data / content while prioritizing other data / content. For example, an internet company allowing users to stream videos from its own sites, while blocking or slowing down video streaming from its competitors, would violate net neutrality. Essentially, it means that consumers should have equal access to the websites, content, and information they want -- that the internet service providers must be an impartial conduit for information.

The Problem:
Net neutrality protects civil rights such as the free exchange of ideas, promotes competition, and ensures small technology companies and other businesses have a fair shot at reaching consumers. A broad net neutrality order was struck down by the Republican-controlled Federal Communications Commission in 2017.

Ross's Solution:
It is imperative that we keep the internet free and open, and ensure net neutrality through federal legislation to ensure Americans are able to decide for themselves what they see, read, and do online.
In addition, as the big technology platforms have increased in power, size, product offerings, and the amount of user data collected, we must recognize that a few key companies have become the gateways the majority of consumers use to access the internet. Therefore, we should examine how to expand net neutrality to also include legislation requiring "platform neutrality." Platform neutrality means that an online platform can not discriminate against other services in favor of its own products or services. This would ensure that when a consumer uses Google Search to look for products to purchase online, for example, Google does not block access to competitors to only show Google's own shopping services. This will ensure that the free market economy that Americans enjoy offline also exists online.