



December 21, 2018

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Room CC-5610 (Annex C)
Washington, DC 20580

Docket ID: FTC-2018-0098-0003

Dear Chairman Simons, Commissioner Phillips, Commissioner Chopra, Commissioner Slaughter, and Commissioner Wilson:

On behalf of National Taxpayers Union's (NTU) thousands of supporters across the country, I am honored to submit the following comments on the Federal Trade Commission's (FTC) upcoming Hearing on Competition and Consumer Protection in the 21st Century, focusing on privacy issues.

Consumer data privacy regulations are an issue of particular importance to Americans right now, but governments across the globe have been taking massive anti-consumer steps in overregulating how the government treats private data.

National Taxpayers Union has been warning against European-style data regulations for years, and we have recently seen the damage that can be done when the European Union instituted its General Data Protection Regulation (GDPR). Secretary of Commerce Wilbur Ross stated the GDPR has [made the EU less competitive](#) and closed off the ability of many EU companies to do business internationally. GDPR has also [killed off a number of small businesses that did not have the resources or the staffing capabilities to comply with the new regulations](#).

A light-touch regulatory regime has worked well for Americans for decades, and the FTC would be forward-thinking to continue this approach. As NTU [commented to the FTC in August](#), the tendency to overregulate can not only impact consumers in negative ways, it can also adversely affect taxpayers.

It is the taxpayers' interest in privacy regulation that will occupy the remainder of these remarks.

Remember the Not-Too-Distant Past. A useful exercise in examining the current state of privacy regulation is to review the past, especially the FTC's activities under former Chair Edith Ramirez. During her first major public interview with the International Association of Privacy Professionals in March 2013, Chair Ramirez defended the agency's more aggressive stance on privacy of consumer data online but also [tried to reassure](#) those in the business community that it was "not a blank check for the FTC in going after privacy violations." In a carefully-worded (and closely followed) August 19, 2013 address before the Technology Policy Institute's Aspen Forum, Chair Ramirez described the FTC's role in the emergence of a data-driven consumer economy as that of a "lifeguard" – one that

would not “spoil anyone’s fun” but would instead “make sure no one gets hurt.” Among the [details](#) of her speech:

- Chair Ramirez recounted the FTC’s dozens of separate data security actions and urged companies “to follow the three core principles laid out in the FTC’s 2012 Privacy Report.”
- Chair Ramirez also called on Congress for greater powers, including repeal of the “common carrier” exception to the FTC’s jurisdiction (thereby giving the entity greater authority over telecom providers) and allowing the FTC to impose civil penalties against firms that fail to provide “reasonable” security of customer data.
- Chair Ramirez issued a short but sweeping cautionary note against “the indiscriminate collection of data,” boiling down her thought into what she called a “commandment” that “thou shall not collect and hold on to personal information unnecessary to an identified purpose. ...And remember, not all data is created equally. Just as there is low quality iron ore and coal, there is low quality, unreliable data. And old data is of little value.”

The impact of this address – billed as a major shift in policy – was at the time difficult to overstate. Alan Friel, an attorney experienced in privacy issues, [wrote](#) in *Advertising Age* that the contents of Ramirez’s remarks “suggested not recommendations of best practices or industry guidance, but what could be interpreted as mandates for industry.” Friel asserted that key words from the FTC Chairwoman seemed to be making a case for consumer harm (and therefore utilization of Section 5 authority). Friel’s advice to businesses was that “companies should be looking at the FTC’s privacy best practice expressions, such as in its 2012 Privacy Report or else be prepared to challenge them as less than required in a potential unfairness enforcement action.”

Of equal weight – and worry – to high-tech economy expert Adam Thierer of the Mercatus Center was the message Chair Ramirez seemed to be sending about significantly narrowing the applicable uses of data. He [noted](#):

[T]he cornucopia of innovation information options and opportunities we have at our disposal today was driven in large part by data collection, including personal data collection. ...For example, many of the information services and digital technologies that we enjoy and take for granted today – language translation tools, mobile traffic services, digital mapping technologies, spam and fraud detection tools, instant spell-checkers, and so on – came about not necessarily because of some initial grand design but rather through innovative thinking after-the-fact about how preexisting data sets might be used in interesting new ways.

By Thierer’s estimation, Chair Ramirez’s speech pushed the FTC even closer to embracing the “precautionary principle”: that in the absence of positive, copious proof a new technology or innovation is harmless to privacy or some other policy concern, public authorities should prevent or discourage its development. Such an approach, if re-applied today, would concern taxpayers as well. Many of the technologies developed from data innovation that Thierer cites above have direct relevance to making government operations more efficient. Mobile traffic services save fuel for government fleets and time for drivers, while digital technologies can assist with making more accurate maps that help to determine premium rates for taxpayer-backed flood insurance in higher risk areas.

NTU would urge Commissioners to regard the events of 2012 and the innovation sector’s reaction to them as a cautionary tale. There are other examples as well, from the European continent.

European Privacy Policy: No Model for U.S. Taxpayers. Europe’s antitrust laws are indeed more onerous than in the United States, as are personal privacy directives (which, to be fair, are rooted in the continent’s experiences of World War II and the Communist Era). Yet apparently, they do not prevent concentration of industrial power in the hands of one entity: government. Europe is littered with examples of state-owned or state-supported enterprises that enjoy subsidized competition against private U.S. companies. These would include airlines, telecommunications concerns, energy firms, banks, and postal services.

As with state-owned enterprises, EU countries continue to exhibit a certain degree of hypocrisy in privacy rules by exempting many categories of government activity. This contradiction is not completely lost on citizen advocates in the region, who for several years [had pressured](#) their governments to revise a Data Retention Directive (DRD) that allows member states to gather and keep all kinds of information from telecom and Internet providers on residents that would be “proportionate to the general interest” (e.g., national security). In 2013 Phil Zimmermann, inventor of the PGP encryption service and founder of the Smart Circle mobile encryption company, [told *Forbes*](#) his firm was setting up servers in Switzerland to steer clear of EU’s data retention laws. He called those strictures “worse than the U.S.”

In addition, the heavily litigated “right to be forgotten” carries with it other concerns for taxpayers. Could politicians with track records of misusing tax dollars have embarrassing facts erased? Does the right to privacy trump the right to free expression? What about the deletion of information that protects public safety? The controversies continue across the Atlantic, even as citizen-based transparency movements in the United States are seeking more, not less, access to data on the way government works.

There are other questions of direct relevance to fiscal and trade policy. As Carl Szabo, Policy Counsel for NetChoice, [pointed out](#) in *Roll Call* several years ago, both Spain and Germany have instituted taxes on search engines and news aggregators that link to media articles. He stated that “While many argue privacy concerns and revenue generation motivate these actions, a fundamental motivation has to be limiting the dominance of U.S.-based Internet companies in Europe.” Today, many would argue that various forms of [digital taxes](#) being pursued at the OECD, EU, and individual nation levels go hand-in-hand with other strictures such as GDPR in order to assert more control over the digital economy itself.

European-style privacy practices present equally daunting prospects for maintaining the vitality of the tech sector. Shortly after the release of FTC’s 2012 Privacy Report outlining the Commission’s preferences, the Information Technology and Innovation Foundation (ITIF) [responded](#), “Consumers should have options to protect their privacy but there are important trade-offs and costs in creating those protections. The FTC’s recommendations would create economic burdens that could stifle the efficiency and innovation that consumers also want from the Internet.”

But how? ITIF’s Daniel Castro connected the dots for Congress a full two years before the FTC’s privacy report, when he testified before a hearing of the House Energy and Commerce Committee on “Do- Not-Track” legislation. The proposal would have created a government mechanism blocking all data profiling in the private sector for advertising purposes (but allowed the government itself to keep doing so for its own uses). Castro recounted how huge swaths of Internet services, from Facebook to YouTube, are free to users precisely because they are supported largely by advertising. He warned that this type of regulation would mean “not only fewer websites and less valuable content, but also less spending by Internet companies on servers and bandwidth. The net result will be fewer jobs.”ⁱ

Backing up these expert opinions are some solid economic projections. Castro's testimony cited a [study](#) by Avi Goldfarb of University of Toronto and Catherine Tucker of MIT, which found that the EU's Privacy and Electronic Communications Directive (promulgated in 2003 following the original 1995 Data Protection Directive) decreased online advertising effectiveness by two-thirds relative to that of the environment in the rest of the world.

A [subsequent analysis](#) by Josh Lerner of Harvard University discovered that the Privacy and Electronic Communications Directive led to a \$249 million decrease in venture capital investment toward European online entrepreneurs in an 8-1/2 year period. However, because venture capital often delivers a greater "bang for the buck," he concluded that "this may be the equivalent of approximately \$750 million to \$1 billion in traditional R&D investment." Several studies since then, (e.g., [Anja Lambrecht](#) in December 2017) have drawn similar conclusions.

Another less quantifiable impact from Euro-regulation could be a ramp-up in a malady that already afflicts parts of American industry: crony capitalism. Milton Friedman identified a "suicidal instinct" in some U.S. businesses when they seek to aim government regulators at their rivals. In his [dissent](#) to the FTC's 2012 privacy report, FTC Commissioner Rosch raised a similar point:

'Unfairness' is an elastic and elusive concept. What is 'unfair' is in the eye of the beholder Not surprisingly, large enterprises in highly concentrated industries, which may be tempted to raise the privacy bar so high that it will disadvantage rivals, also support adopting more stringent privacy principles.

Some would argue that a central problem underlying identity theft is the lack of privacy protections built into the services and products of firms like Facebook and Google. Yet, governments themselves have dismally failed to lead by example. Chief among these is the IRS, which both the Government Accountability Office (GAO) and the National Taxpayer Advocate have cited for shortcomings in identity theft protections and resolution procedures.ⁱⁱ

Federal policy toward the privacy of taxpayers is likewise deficient, and in our opinion could do far more financial damage on a case-by-case basis than a given private-sector company's treatment of a consumer. The 32-year-old Electronic Communications Privacy Act permits government entities to access an individual's personal data after it has been stored for 180 days. While typically viewed as a prerogative of traditional law enforcement agencies, apparently the [IRS can avail itself](#) of a taxpayer's information under this policy, even if such information has no direct bearing on a specific, active investigation.

Data Innovation=Government Innovation. Despite some spectacular hardware failures, "e-government" has delivered clear efficiency and effectiveness dividends to taxpayers, at all levels. Few of these dividends would ever have been realized in a restrictive policy environment that prevented the evolution of new data-driven consumer and business-to-business services that could be adapted for government's use. Data sharing of the kind that former Chair Ramirez raised concerns about can actually help to combat government waste in several ways, such as preventing improper payments to those who are deceased or incarcerated. The emergence of "[smart card](#)" technologies could, if applied government-wide, reduce losses to fraud and misapplied entitlement cases by several billion dollars annually.

For more than a decade the White House has made [annual reports to Congress](#) on e-government initiatives throughout the federal bureaucracy. A few examples from previous reports include:

- The National Contact Center, a multimedia federal portal for citizen questions about benefits and for interagency communication, delivered some \$200,000 in savings to the Fish and Wildlife Service alone by providing speedier assistance with inquiries about permits and other administrative matters.
- The Federal Emergency Management Agency replaced its decades-old content management system with a “cloud”-based alternative that helped the agency re-launch websites in 2011 and 2012. The system cost \$1.4 million, but is delivering \$220 million in savings over five years.
- The HR Line of Business program began a government-wide transformation of human resources information technology by focusing on modernization, integration, and performance assessment. A key element is the use of “shared service centers” that all agencies can access. Projected savings amounted to \$1.6 billion through the year 2015.

End-users of “e-government” benefit from the quality of service as well. NTU has [lauded the success](#) of the IRS Free File program, a public-private partnership for federal tax return preparation and online filing. The initiative has saved \$1.5 billion since its inception in consumer expenses as well as government costs normally incurred through processing paper returns.

The current Administration’s [government management plan](#) leans heavily on technologies and methods developed in the private sector. The Office of Management and Budget reports that the use of Technology Business Management techniques from FY 2015 through FY2017 have resulted in a four-fold increase of federal IT spending that “could be clearly tracked to a specific cost category” – an essential element of any plan to ensure that budgets for these activities are rightsized. Again, a key to the success of the White’s House proposed “Technology Modernization Fund” will be fast adoption and adaptation of IT solutions first born in the private sector.

Nor are benefits like these confined to the federal level. NIC, a private technology provider, lists numerous [“case studies”](#) on its own website of how state and local governments (and in turn taxpayers) reaped rewards from technology as well. Solutions ranged from online vehicle recordkeeping, to procurement tracking, to business form filing.

But perhaps the most important transformative technology for government in recent years has been the use of cloud-based data management and communication services. In 2011, NTU partnered with the U.S. Public Interest Research Group to [produce a report](#) for Congress’s deficit reduction “Super Committee. One key recommendation of the report was to implement federal IT management reforms:

Taking advantage of options such as virtual network-based computing technology while closing up to 800 of the 2,100 federal data centers nationwide, as proposed by the Obama Administration, would save taxpayers an estimated \$160 billion over the coming decade.

While follow-on estimates were less optimistic, the use of data-driven innovative models in the private sector is still revolutionizing the way government spends taxpayer funds on information management. The cloud-based [Joint Enterprise Defense Infrastructure Project](#), currently in progress at the Department of Defense, is just one such instance.

It is clear that hi-tech innovation can change the quality and cost of government for the better, if federal managers properly embrace it. Yet, they may have fewer opportunities to do so, if the pipeline of private-sector development is slowed or cut off due to government regulatory overreach.

Conclusion: Taxpayers Are Best Served by Balanced Privacy Policies. NTU has presented much of the material in these comments to Commissioners in other settings and hearings, but it bears repeating because the interests of taxpayers in sound FTC policy is not necessarily as evident as it should be. Furthermore, recent history remains an excellent guide for policymaking even with what appears to be a constantly-evolving tech sector.

It is our hope that the observations outlined above will continue to be of assistance in FTC's deliberations. All of you are to be commended in providing the most comprehensive exploration of antitrust, competition, privacy, and other matters of interest to the FTC in more than two decades. Thank you for your consideration, and should you have any additional questions, I am at your service.

Sincerely,

Pete Sepp
President

Notes

ⁱCastro, Daniel D., “‘Do-Not-Track’ Legislation: Is Now the Right Time?” Information Technology and Innovation Foundation, Testimony before the Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce, December 2, 2010.

ⁱⁱ See, for example, Internal Revenue Service National Taxpayer Advocate, “Most Serious Problems Facing Taxpayers: Identity Theft Victim Assistance,” *2013 Annual Report to Congress*, January 2014. <http://www.taxpayeradvocate.irs.gov/2013-Annual-Report/id-theft/>. The Advocate's follow-up “Report Card” on remedial recommendations for identity theft reported partial progress in most areas. http://www.irs.gov/pub/tas/2013ARC_ReportCard.pdf (see pp. 29-43).