August 24, 2017

Via Electronic Submission to https://ftcpublic.commentworks.com/ftc/canspamrulereview

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20024

RE: CAN-SPAM Rule, 16 CFR Part 316, Project No. R711010

To Whom It May Concern:

When The Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) was enacted in 2003 we never could have foreseen that the use, or the abuse for that matter, of email would grow to today's levels. The compromise of individual email accounts makes national headlines and may be responsible for the swaying of elections. In the early 2000's it was impossible to imagine how security technology would affect the implementation and distribution of email, but in today's world securing email communications and the brands that send them are part and parcel of doing business on the internet. Our concern at the time was keeping email a vital and used channel regardless of whether or not we could come to a collective agreement about the level or type of control, policy or technology, that would ensure email's use, growth and utility.

Fifteen (15) years on we are dealing with the exponential growth of bad actors to the extent that privacy issues are now driving policy decisions in a futile attempt to prevent massive, wide-scale abuse. As it stands, the United States remains one of the very few countries in the world that favors opt-out laws for the use of personal information, including email addresses, within a fragmented and sectorialized privacy and data protection regime. The rest of the world requires permission from the data subject in order to collect and process Personally Identifiable Information (PII), which generally includes email addresses. We do know that opt-in requirements in Canada's Anti-Spam Law (CASL) and the E.U. Data Protection Directive (Directive 95/46/EC) have both been successfully implemented without creating significant business disruptions or negatively impacting either economy. In fact, the move to this requirement was shown to foster trust in those collecting and processing personal data. Furthermore, businesses outside of those two geographies are required to comply with those frameworks when attempting to digitally communicate with customers and subscribers (data subjects) that live there.

What we have learned over the years is that while many of organizations that are interested in the legitimate use of email as a marketing tool abd many have abided other self regulatory models, the only individuals for whom a self regulatory model works are companies that understand the value and importance of constraint and good behavior. Bad actors can not be coaxed into doing the right thing with a carrot, such as preferred mail handling or inbox placement. As a result, ISPs and the operators of blacklists have developed punitive measures in response to escalating abuse. For rogue organizations, and in light of the shifting global attitude toward individual privacy, a higher regulatory standard is required to modify behavior, protect the rights of end users who find more and more of their personal data surfaced on the internet, and are preyed upon by not only those that operate in the shadows but unscrupulous companies unconcerned by the erosion of self regulatory controls and mechanisms.

Because of the fast pace of changes, and the rise in abuse of the email channel, I am advocating that the Federal Trade Commission (FTC) consider in any report sent to the U.S. Congress that CAN-SPAM be reviewed for the consideration of amending the law from Opt-Out to Explicit Opt-In when it comes to the primary purpose of an electronic mail message for commercial electronic communications. I am not advocating for changes to how a transactional message is regarded or treated under the current CAN-SPAM framework, only that commercial email permissions be amended to an Opt-In framework.

While it is still likely that only those responsible organizations will step up to the higher standard required by an opt-in rule, that simple change will make it easier for our regulators, ISPs, Attorneys General, and consumers to differentiate “good” mail from “bad” mail. It will also bring our electronic policies more in line with other leading nations.

Similarly, I feel that a move to an opt-in standard would provide a more unified enforcement standard globally. Many nations already have opt-in standards in their federal regulations: Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's Anti-Spam Law (CASL) and the E.U. Data Protection Directive (Directive 95/46/EC), are just a few of the many examples of national opt-in standards. Others, like France (opt-in for direct marketing by e-mail), Germany (opt-in for telemarketing), and Australia (Spam Act 2003) require commercial electronic messages--including email, instant messaging, SMS, and MMS--to be sent with the prior consent of the recipient, unless there is an established business relationship.

I recognize the burden that it may put on certain companies that have operated at the margins of the self-regulatory frameworks. However, as an organization dedicated to ensuring the long term viability of the channel, protecting individual rights and tightening the policy surrounding commercial email is part and parcel of recognizing email’s importance in today’s marketing world. Today, more than 4 billion global users depend on the utility, reliability, accessibility, and

ubiquity of email - a level of adoption no one would have anticipated. As a result of the near universal nature of email, it has evolved simultaneously into the most open communications platform as well as the most abused channel. The fact of the matter is that as an indivdual I care deeply about Email and believe that policies governing the data collection mechanisms need to evolve to better fit its use in the modern world.

Sincerely,
Dennis Dayman