

Killi Ltd: How Privacy Will Upend Advertising in 2021

Killi featured in Street Fight discussing the expected impact of privacy laws on advertising and consumers.

New York, New York--(Newsfile Corp. - January 21, 2021) - [Killi Ltd.](#) (TSXV: MYID) (OTCQB: MYIDF) ("Killi"), a global leader in data and consumer privacy, is featured in [Street Fight](#) providing commentary on changing privacy laws and the mobile solution to identity.

In the new age of privacy compliance, we see a confusing set of laws and proposed solutions that are not only incongruent but short-sighted. Consumers can't be confident at this stage that their identities are protected, even with growing legislation, and advertisers are scrambling to uncover the future state of consumer IDs with little confidence. In short - both advertisers and consumers are set for significant disruption in 2021, across state lines and international borders.

Existing government regulation

In 2018, the EU's GDPR went into effect, levying massive fines against violators of its privacy guidelines and spawning a movement of companies abroad returning to the US to avoid strict regulation. While dumping the EU was convenient for US-based firms, international companies have not been so lucky. These firms have been named in class-action [lawsuits](#), most notably the \$10B suit against Oracle and Salesforce.

Yet even domestically, there is a growing fear of violations, and websites hosted by brands and advertisers alike have been quick to adopt pervasive pop-ups that enable consumers to allow or deny the use of cookies while browsing. As privacy awareness has grown, we've seen acts like the CCPA and CPRA pass at the state level, modeled after the "gold standard" of GDPR's policies. Again, it's likely that companies will continue to flee areas that pass such strict regulations to avoid litigation in favor of states that pledge no such action. But how long until the federal government intervenes?

Big Tech's Ploy

Amid the dust that's been kicked up by the whirlwind of policy, data giants like Google, Apple, and Facebook are beginning to tout themselves as champions of consumer privacy. They're creating the public perception that their solutions for mobile IDs and hashed email are the future of security and the path forward from the demonized cookie.

However, a peek behind the curtain would reveal that all of this noise showcasing their altruistic endeavors is just a mask: The data giants are orchestrating a move that will massively benefit themselves. Should these walled gardens win out, advertisers and publishers will be forced to use these platforms for not just any but *all* advertising placement. Audiences will be the sole property of each of the big players, who will take their share of the ad revenue they fully control. The ad industry will have no choice but to bend to their will, and these private exchanges will be able to control the full gamut of participation from pricing models to audiences.

Providers Turn to Email

It sounds terrible because it is. It's why the IAB is working on its own Project ReArc to develop a universal tracking ID to prevent Big Tech's takeover from happening. The IAB has always fought for a single set of standards that protects both the consumer and the advertiser, which would be negated should the data giants win. It's promising in its premise, but there's one flaw with all of these solutions: The IAB is also determined to use hashed email as an identifier.

Other solutions in the market are not as altruistic as Project ReArc and have a higher probability of gaining traction. Not surprisingly, these are led by companies who stand to lose the most from the cookie's depreciation. The Trade Desk and LiveRamp's ATS solutions are currently the frontrunners and seem to be separating themselves from the pack. These solutions' weakness is the same as the others: The Trade Desk and Liveramp also use email as their core identifiers for their ID solutions.

Why is this a problem? Well, for starters, both personal and professional communication has taken the form of Slack, TikTok, Zoom, and their many social media counterparts. All of these platforms limit the scope of email's penetration across consumers. The younger demographic almost exclusively uses alternative channels to communicate and are likely to do so as they mature. Email is an inadequate means of tying together online and offline events, making attribution a muddled guessing game. Furthermore, the EU is likely to block email as an identifier, and we've seen how quick we are to adopt such policies domestically.

The mobile solution to identity

So, while the walled gardens continue to champion hashed emails because they're easy to own in their environment, the one solution that solves for advertisers and consumers alike is being overlooked: the mobile number. Mobile numbers are pinned to devices themselves, which [the average adult has more than three](#) of. Consumers own them, and better yet, these are a function of wireless carriers - regulated by the FTC.

A bonus? The [vast majority of Americans - 96%](#) - now own a mobile phone. By contrast, [only 76% of US adults use email](#), with email usage tapering off in younger generations.

For advertisers, mobile number adoption as an ID solution means universally accepted, privacy-compliant tracking. Advertisers will have relationships with publishers directly and through ad networks instead of working through the data juggernauts as middlemen. Free enterprise would persist, the IAB could maintain fair governance, and attribution could be ensured across online and offline touchpoints. For consumers, peace of mind would be restored because the FTC will broadly regulate privacy and security. And we consumers can once again benefit from a personalized browsing experience, both in the websites we navigate and in the ads shown to us. The internet can be exciting and engaging to us no matter where we surf.

Why confusion will persist

Of course, if mobile numbers are adopted, Apple, Google, and Facebook won't get their way. They will not go down quickly and will likely continue to bury email IDs as a viable solution. We'll see the entire industry disrupted as each of the powerhouses marches forward with their plans to own the future of privacy, ensuring they monetize the very thing they are touting to protect. Advertisers will be forced to evolve targeting strategies, tackle new CDP hurdles, and upend their media strategies to conform to disparate and confusing practices. Consumers will still live in a world of privacy uncertainty. All the while, states will continue to legislate while companies relocate to avoid prosecution - all for a consumer ID solution bound to change once again.

For now, it seems we are barreling down a futile path, but it's a temporary one. Let's hope the IAB and other regulating bodies can intervene fast enough to prevent the massive disruption that awaits us.

[Neil Sweeney](#), CEO and founder, Killi

About Killi

Killi is a consumer privacy ecosystem that allows consumers to take back control of their consumer data from those who have been collecting it and selling it unbeknownst to them. Killi is currently available online or via [iOS](#) or [Android](#) in five countries (US, Canada, Singapore, Australia, and New Zealand). Killi pays users automatically every week a cash Data Dividend™ for the use of their data, making Killi the

only company in the world that is fairly compensating users for the purchase of their data. Killi is also the creator of uaretheproduct.io, a consumer-facing website that allows consumers to determine their data's value broken out by individual platform.

To learn more about how Killi fairly pays users via its [Fair-Trade Data](https://killi.io/earn)TM program, please visit <https://killi.io/earn>.

Download Killi [here](#).

FOR FURTHER INFORMATION, PLEASE CONTACT:

Andrew Elinesky, CFO
+1-416-904-2725

Neither TSX Venture Exchange nor its Regulation Services Provider (as that term is defined in policies of the TSX Venture Exchange) accepts responsibility for the adequacy or accuracy of this release.

Forward-Looking and Other Cautionary Statements

This news release may contain "forward-looking statements" within the meaning of applicable securities laws, including, but not limited to, significant disruption in the data and/or tech industry in 2021, the efficacy of proposed solutions to new privacy laws, tech incumbents continuing to use email IDs, advertisers being forced to evolve targeting strategies, tackle new CDP hurdles, and upend their media strategies to conform to disparate and confusing practices, main consumer ID used by the industry bound to change again. Forward-looking statements may generally be identified by the use of the words "anticipates," "expects," "intends," "plans," "should," "could," "would," "may," "will," "believes," "estimates," "potential," "target," or "continue" and variations or similar expressions. These statements are based upon the current expectations and beliefs of management. They are subject to certain risks and uncertainties that could cause actual results to differ materially from those described in the forward-looking statements. These risks and uncertainties include, but are not limited to: constantly changing privacy laws, extensiveness of scale and international coverage; the uncertainty surrounding the spread of COVID-19 and the impact it will have on the Company's operations and economic activity in general; and the risks and uncertainties discussed in our most recent annual and quarterly reports filed with the Canadian securities regulators and available on the Company's profile on SEDAR at www.sedar.com, which risks and uncertainties are incorporated herein by reference. Readers are cautioned not to place undue reliance on forward-looking statements. Except as required by law, the Company does not intend and undertakes no obligation to update any forward-looking statements to reflect, in particular, new information or future events.

This press release does not constitute or form a part of any offer or solicitation to purchase or subscribe for securities in the United States. The securities referred to herein have not been and will not be registered under the Securities Act of 1933, as amended (the "Securities Act"), or with any securities regulatory authority of any state or other jurisdiction in the United States, and may not be offered or sold, directly or indirectly, within the United States or to, or for the account or benefit of, U.S. persons, as such term is defined in Regulation S under the Securities Act ("Regulation S"), except pursuant to an exemption from or in a transaction not subject to the registration requirements of the Securities Act.

Neither the TSXV nor its Regulation Services Provider (as defined in the TSXV Manual) accept responsibility for this news release's adequacy or accuracy.



To view the source version of this press release, please visit

<https://www.newsfilecorp.com/release/72528>