Toluna

DATA QUALITY AND SECURITY BEST PRACTICES

DATA QUALITY WHITE PAPER

MAY 2018

GLOBAL CLIENTS OF ALL SIZES AND INDUSTRIES PARTNER WITH TOLUNA AS THEIR ALL-IN-ONE PROVIDER FOR ACTIONABLE CONSUMER INSIGHTS BECAUSE THEY KNOW THAT WE TAKE PROACTIVE MEASURES TO ENSURE THAT WE'VE TAKEN AN IRON-CLAD APPROACH TO SAFEGUARDING THEIR DATA.

Furthermore, the market research industry is especially susceptible to hacking (with the intention of gaming the system for an additional incentive, or rewards), and/or business abuse (with an intention of targeting businesses, and doing harm). "Bots" in particular have begun to pose new challenges, as they aim to complete surveys automatically, and we've seen them bypass tried and true data quality best practices.

As always, Toluna takes a sophisticated, leading edge approach to data quality, and security best practices.

NEXT GENERATION THREATS ARE PREVENTABLE WITH A NEXT GENERATION SOLUTION

Toluna is pleased to announce a partnership with CDNetworks, to use its Web Application Firewall (WAF). The CDNetworks WAF is an intelligent, multi-layered approach to data security. The cloud-based solution is a global, 24x7 industry-leading, next generation technology that is self-learning and self-evolving.

CDNetworks Cloud Security WAF provides the following defenses:

Spam and Abuse Protection	A set of rules to prevent spam and abuse of websites forms.
CMS Platforms Protection	A set of rules and tools to fortify popular web CMS systems.
Application DDoS Protection	Protection against attempts to knock down websites with layer-7, DDoS, such as HTTP-Get floods, Slow Loris, Rudy and others.
WAF (SQLi, XSS & More)	A first layer of defense against hacking attempts such as SQL injections.
Cross Site Scripting (XSS)	and others by both human and non-human (BOTS).
Reputation Firewall	Blocking Traffic from IPs known to be dangerous or malicious.
Screen Scraping Protection	Protects websites against screen scraping and bot crawling.
Behavioral WAF	Behavioral user risk assessment to block malicious bots and high-risk sessions. Blocks low-and-slow DDoS attacks, password brute-forcing, probing and attack planning by hackers and servers to add power and resilience to all other security layers to mitigate sophisticated attacks.

We leverage this solution across our registration practices, individual surveys, our on-site, Toluna.com activities, and third parties.

A CONTINUED FOCUS ON REAL, VALID, DE-DUPLICATED, ENGAGED AND REPRESENTATIVE RESPONDENTS

Toluna's member recruitment practices focus on ensuring that all recruitment investment leads to quality respondents who participate in our surveys. Respondents who are recruited into the Toluna community undergo a series of quality checks, and our goal is to ensure respondents are Real, Valid, De-Duplicated, Engaged and Representative.

The following outlines the steps taken to ensure data quality.

Real – ensuring respondents are in fact 'real' people

GeoIP and postal-code-validation programs	Used as a means of validation to ensure registrants provide information that is correct. For example, individuals who provide an incorrect zip or postal code based on other address details should be excluded.
Imperium's Address Correct®	Integrated with our survey systems and prevents individuals from participating in surveys unless valid postal addresses are used.
CAPTCHA	A program intended to distinguish human from machine input, which asks users to enter a unique, automatically generated confirmation code upon registration.
Web Application Firewall (WAF)	Toluna licenses this cloud-based service from CD Networks, and obtains protection against hacking, business abuse and malicious attacks (aka "bots"). This protection is used upon member registration, Toluna.com, and individual surveys.

Valid – individuals are knowingly joining Toluna's community, participating in surveys

Individuals must double opt-in

Members confirm membership by clicking on an emailed link upon completion of the Toluna enrollment survey.

Members must complete a survey to complete membership

Imperium's Verity®

A third party identity validation service is used to confirm survey respondent's name and address against third party databases to ensure identity.

RelevantID™ Fraud Profile Score

Compares a user's machine and operating system time zone and language settings to Geo-IP location to detect discrepancies and deny survey entry to machines with suspect fraud markers. Also provides bot , Tor Network, Proxy/Data Center IP address, browser tampering & device emulator detection.

De-Duplicated – individuals can't take surveys more than once, knowingly, or unintentionally

Toluna's proprietary Duplicate Respondent Detection™	A cookie-based technology used during the member registration process to ensure there are no duplicate respondents within the community.
Imperium's RelevantID™	A third-party digital fingerprinting technology that prevents respondents from participating in surveys more than once intentionally or non-intentionally.
Additional de-duplication checks	Toluna uses technology to produce a proprietary matching algorithm to flag similarities of new registrants with existing Toluna.com members.

Toluna ensures engagement and representativeness on an ongoing basis by leveraging best-practices approaches for straight lining, red-herring implementation, and more.

APPENDIX: TYPES OF BOT ATTACKS WE'VE SEEN AND PREVENTED

Category	Typical Attack Type	Description of Attack	Possible Damage
Hacking	SQL Injection(SQLi)	Sending SQL commands to vulnerable web applications	Data breach, fraud, defacing or shutting the website down
	Cross Site Scripting(XSS)	Injecting Browser code	Malware Infections, data breach
	Session Hijacking	Posing as another user	Data Breach, Fraud
Business Abuse	Screen Scraping	Systemically copying a website's public data and contents	Negative impact to the business competition, customer harassment
	Form Spamming	Posting to web forms with spam	Business disruption, links to malware
	Fake Accounts	Creating multiple fake accounts	Fraud, using platform for spam purposes, negative impact to credibility and nrand value
Denial of Service	DoS/DDoS	Knocking down a website	Business Interruption and negative impact to credibility and brand value

Toluna

E toluna@toluna.com **T** +1 203 834 8585 **W** corporate.toluna.com