Protecting User Privacy is Not Optional

Online services face increasing public pressure to protect their visitors' private data. This is reflected in many new data privacy laws around the world.

Headlines tell us daily of new data breaches and enormous losses of sensitive Personally Identifying Information ("PII"). While the need to protect user data from cybercriminals is increasingly obvious, online services must also ensure their policies, partners, and practices minimize data collection and safeguard PII.

In this article we'll look at how ***hCaptcha*** helps to protect PII from outside attackers and unintentional abuse within your organization.

hCaptcha
Enterprise

The Leading Security ML Platform for Fraud and Abuse

How is User Privacy Compromised?

Outside Attacks on User Privacy

Online fraudsters use many techniques to discover, steal, abuse, and otherwise compromise user privacy. The use of bots to provide automation is a vital and common ingredient among these techniques. Because bots are so heavily used by attackers, their very presence is a key indicator of a potential attack that could compromise user privacy. To understand this, let's look at how fraudsters operate to steal and exploit PII. Two methods are common: Account Takeovers (ATO) and New Account Fraud.

ATO Attacks - A Direct Assault on User Privacy

In an ATO attack, fraudsters often use an approach called credential stuffing. The technique utilizes bots to automatically inject stolen user IDs and passwords into login forms. The goal is to give the attacker access to, and control over user accounts. Successful ATO operations can be very damaging to victims, who not only lose control over their accounts, but also their PII. Depending on the type of site, fraudsters can obtain vast amounts of sensitive personal data with each successful login.

New Account Fraud - Abusing Previously Obtained Private Information

New account fraud, or ***fraudulent account registration***, is another common attack. Bad actors obtain stolen personal data, including login credentials via the dark web or another unsavory channel. As with an ATO attack, these bad actors then use bots to automate their attack, rapidly filling out new account forms with the stolen PII. The fraudulent accounts are used to make purchases, ***generate spam***, spread misinformation, distribute malware, scrape PII from social media and other sites, and perform a host of other nefarious deeds. Any of these activities can be extremely harmful to the victim.

Automation: A Key Ingredient for ATO, New Account Fraud, and Other Attacks

As described in the ATO and New Account Fraud examples above, automation is a key tool in an attacker's arsenal. Without bots, many cyber crimes are too labor intensive to be profitable. Because bots are readily available, relatively inexpensive, and don't require a great degree of skill to use, fraudsters turn to them to carry out their attacks.

Due to the prevalence of bots in cybercrime attacks, it's critical for website applications to quickly and accurately differentiate between ***malicious bot*** and legitimate user traffic.

Business Abuse of PII and User Privacy

In the section above, we discussed how PII can be illegally obtained by criminals attacking web applications, but PII can also be abused by businesses and other organizations. This occurs when web applications (including partners or vendors) capture, retain, transmit, or otherwise leverage PII without the user's knowledge or express consent.

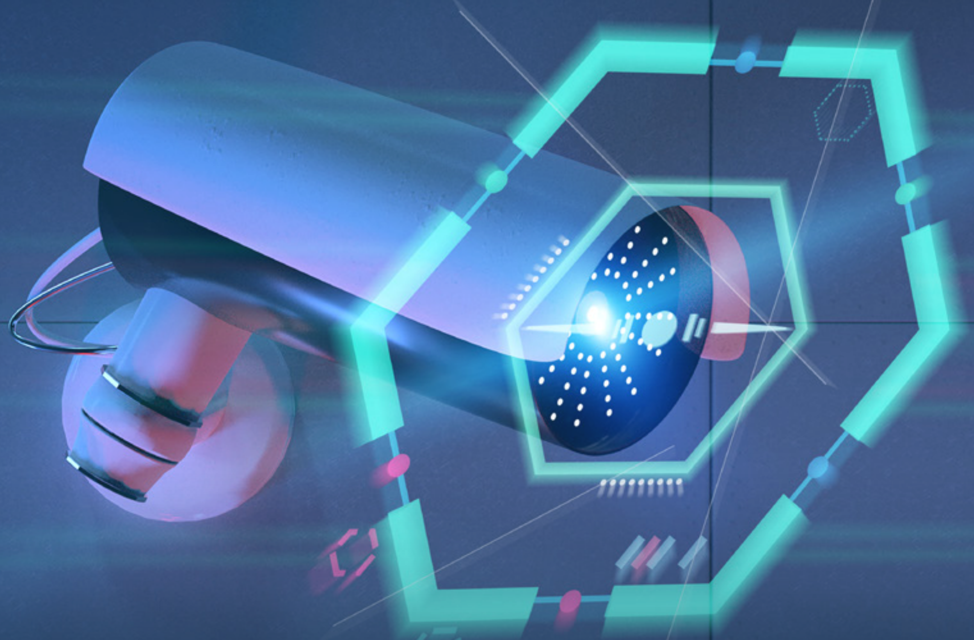
In this scenario, the PII is typically stored in the form of cookies on the user's device, and then transmitted to the website for processing (and sometimes to partners or other third party services the website is utilizing). The information identifies the user and contains data associated with that individual.

Your address, sex, age, the language you speak, the internet searches you've made, the articles you've read, how many clicks you made on a page, site passwords and more are often stored within these cookies.

Although this personal information is obtained by web applications themselves and not by outside criminal attackers, the data still contains PII, and many view its retention and use as an invasion of privacy. This is especially true when that information is transferred to other organizations without the user's knowledge or consent.

The transmission of PII to partners or outside services is a specific concern for websites that are utilizing ***bot detection*** technology. This is somewhat ironic because bot detection is a fundamental solution for detecting PII abuse, and yet many bot detection systems in use today transmit PII between online properties and third-parties for processing. This practice perpetuates the use of PII and may fail to comply with emerging privacy laws in some countries.

hCaptcha processes data close to the user in more than 250 locations and has always focused on de-identifying, discarding and aggregating all data as rapidly as possible, ensuring maximum compliance with privacy laws via our privacy-first design. ***hCaptcha Enterprise*** offers additional safeguards with features like Secure Enclaves and Zero-PII blinding. We are much more interested in technical guarantees than legal ones, and lead the field in privacy-preserving machine learning for security use cases.



The Growing Demand for Digital Privacy

With the prevalence of criminal theft and organizational abuse of PII, the public is taking a much harder stance on privacy protection.

Do Not Track, Surveillance Capitalism, Data Privacy Day (or *Data Privacy Week* starting in 2022) – these and numerous other taglines, mottos, and phrases continue to underscore the evolving attitudes and trends in protecting digital privacy.

Rapidly Evolving Privacy Laws

Driven by demands from individuals and organizations, governments have stepped in to protect private information, passing numerous legislative mandates to restrict its use.

In general, the laws prohibit PII from being collected, retained, or transmitted unless the data is critical to the service being offered, the user has been informed about how their data will be used, and has given consent or accepted that the data processing is necessary for the operation of the service.

Some of the more significant privacy laws affecting online services include the following:

GDPR: The General Data Protection Regulation is a set of online privacy laws protecting residents of the European Union. Any organization that interacts with residents of the EU must comply with the directive.

CA CCPA: The California Consumer Privacy Act regulates the sale of personal information of California residents. This affects everyone doing business with California residents.

LGPD: Brazil's first comprehensive data protection regulation, which broadly aligns with GDPR principles.

COPPA: Mandates that websites that collect PII from children must obtain parental consent before collecting, using, or disclosing children's personal information.

CalOPPA: requires that a privacy policy identify both the categories of personal information that a website collects and the categories of third-party persons or entities with whom the website operator may share that personal information.

PIPEDA: Canada's Personal Information Protection and Electronic Documents Act.

PIPL: China's online privacy legislation, similar to Europe's GDPR but containing additional requirements around data locality.

In addition to these and other existing mandates, new privacy legislation is being developed around the world and the trend shows no sign of slowing.

As governments tackle privacy, it is imperative for businesses to ensure that their practices are in compliance with the numerous existing regulations and those expected to go into effect in the near future.

How hCaptcha Protects User Privacy

Bots are nearly ubiquitous with attacks that compromise user privacy. hCaptcha Enterprise was developed specifically to *mitigate automated threats* while protecting user privacy.

A unique edge-first privacy-preserving machine learning approach rapidly differentiates between bad actors and legitimate human traffic while rapidly discarding PII. This allows organizations to protect data from cybercriminals and potential business abuse, while complying with privacy regulations.

Why Choose hCaptcha to Protect User Privacy?

hCaptcha Enterprise provides customers with optimal accuracy, scalability, and performance, and was designed as a privacy-first solution. Here are some of hCaptcha's privacy advantages:

Private by Design: hCaptcha was designed from the ground up to address online privacy. Other providers have business models that are dependent on PII to serve ads; their technology is built around the need to monetize this online traffic. hCaptcha doesn't care who users are: the goal is security, not selling ads.

Privacy-First Machine Learning: hCaptcha's solutions were built on a sophisticated machine learning platform that accurately and effectively discerns between bot and legitimate human traffic without requiring the retention of PII.

Compliance with Privacy Laws: hCaptcha is compliant with GDPR, CCPA, LGPD, PIPL, CalOPPA, and many other global privacy mandates.

Privacy Pass: hCaptcha is working on initiatives like Privacy Pass, an emerging standard for preserving user privacy being developed via the IETF in conjunction with Cloudflare and other partners.

Data Processed Locally at the Edge: With over 250 locations globally, hCaptcha customers have the option to process requests very close to the user. This provides unparalleled performance and simplifies compliance with privacy mandates around the world.

Ephemeral Data: The data used to analyze visitors to an online property is very short lived and routinely expunged.

No PII Retention: hCaptcha does not retain PII or rely on click-path analysis. It reliably performs an instant evaluation of online traffic beginning from the moment the page is loaded.

Advanced Privacy Options - hCaptcha includes a number of other advanced privacy options such as in-browser firewalls, secure enclave, and other features.

hCaptcha delivers superior bot and fraud detection to organizations that need to stay ahead of evolving threats without compromising end-user privacy.

To learn more about hCaptcha Enterprise, ***click here***.

To request a complimentary pilot, ***click here***.

hCaptcha Enterprise

The Leading Security ML Platform for Fraud and Abuse