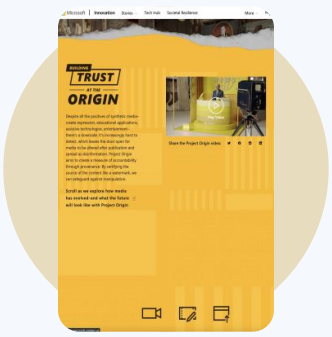


ARTICLE

Building Trust at the Origin

Project Origin aims to create a measure of accountability through provenance: By certifying the source of the content like a watermark, we can safeguard against manipulation.

Microsoft © 2021

Read the article

getAbstract Rating

★ 8 | Concrete Examples | Comprehensive | Analytical

What You Will Learn

- Why digital fingerprints and ledgers help verify media authenticity at the source.
- How Project Origin builds a chain of provenance to combat deepfakes and disinformation.
- Why industry-wide adoption and collaboration are vital for effective media trust tools.
- How media literacy and detection tech empower consumers to spot manipulated content.

Supported Skills

AI Transformation

About the Author

Microsoft Corporation is an American multinational technology corporation which produces computer software, consumer electronics, personal computers, and related services.

Recommendation

In one of its “ALT Stories,” Microsoft introduces “Project Origin,” which seeks to create a “chain of trust” between media content producers and consumers. In a video section of *Building Trust at the Origin,* Microsoft distinguished engineer Henrique Malvar explains how synthetic media, while useful for education, creative expression and more, is too often used for societal and political manipulation. Project Origin proposes an open standard that creates “accountability through provenance,” through which people can authenticate each media source by noting a trusted watermark.

Take-Aways

- As global disinformation proliferates in the 21st century, public trust in media declines.
- Project Origin provides tools for publishers and consumers that identify altered media.
- Henrique Malvar, a Microsoft distinguished engineer, believes that returning trust to news is an essential modern task.
- Today’s widespread media manipulation seeks to defame, persuade and polarize.
- Multiple technologies to detect disinformation campaigns must be widely adopted, and consumers must be educated about them.

Summary

As global disinformation proliferates in the 21st century, public trust in media declines.

In years past, media remained relatively unchanged from publisher to consumer. It was created by professionals and delivered by trusted individuals. Those “closed” information systems allowed people to trust that what was seen and heard was produced by the original publisher.

> *"Despite all the positives of synthetic media…there's a downside. It's increasingly hard to detect, which leaves the door open for media to be altered after publication and spread as disinformation."*

The internet and social media created a decentralized distribution system. Information is redistributed through third-party publishers, then further redistributed through millions of individual consumers. In this environment, disinformation spreads like wildfire on websites, streaming platforms and social media sites. This opens the door for purposely manipulated media, which is often difficult to detect.

Project Origin provides tools for publishers and consumers that identify altered media.

Project Origin's tools give people more opportunities to decide whether information is trustworthy or not – by considering its actual source.

For producers, new tools register media items with a digital fingerprint. Content creators receive a certification of authentication, stored in a tamper-proof distributed ledger that isn't controlled by any single entity. The certification is embedded into media before distribution.

For consumers, web browsers and apps compare the embedded digital fingerprint of files viewed with the original identification stored in the distributed ledger. An authentication display indicates whether the material exists in its original form, or has been altered.

Project Origin's first steps work toward establishing a formal industry standard. Founding members of the Coalition for Content Provenance and Authenticity include Adobe, Arm, BBC, Intel, Microsoft and Truepic. The Coalition's success depends upon wide adoption. Media manipulation is a complex and growing problem. These tools introduce a level of accountability that should help slow the spread of disinformation.

Henrique Malvar, a Microsoft distinguished engineer, believes that returning trust to news is an essential modern task.

Henrique Malvar laments that in years past, traditional news broadcasts were people's "window to the world." Today there are so many screens, people can't believe everything they see.

> *“It’s clear that a healthy democracy requires healthy journalism.” (Henrique Malvar)*

Editing software, computer graphics and AI provide tools for “modifying and synthesizing media.” This causes people to question everything they hear and see, and to find it difficult to separate fact from fiction.

Such technological challenges require innovative solutions. Even slight manipulations of picture and sound can modify intended media messages. “Deepfake” software alters video and photos and presents an especially insidious form of manipulated media. Today’s easy-to-use AI programs allow almost anyone to create highly realistic deepfakes.

Identifying authentic media sources provides “a chain of trust from the publisher to the consumer.” The system doesn’t establish media trustworthiness. It simply identifies publishers by building a “chain of provenance.” To do this work, Project Origin requires commitments from key organizations to adopt an open source standard.

> *“We need expertise from technologies, immediate processing, security, as well as understanding of the publishing processes of news. ” (Henrique Malvar)*

When publishers release media, Project Origin’s tools create a digital fingerprint which is stored in a Cloud service. Its certification of authenticity is retained in the distributed ledger, across multiple servers. In that way, no single entity controls the verification. Similar to a blockchain, these databases are cryptographically secure.

Today’s widespread media manipulation seeks to defame, persuade and polarize.

A recent Princeton study identified 96 foreign influence campaigns from 2013 to 2019. Almost a third targeted the United States, but more than a dozen other countries were similarly attacked. The nefarious campaigns used original and manipulated information to achieve their goals. Disinformation about COVID-19 is thought to have led to unnecessary deaths and hospitalizations.

Microsoft’s Defending Democracy Program helps to protect voters with its ElectionGuard initiative. It also employs Microsoft 365 for Campaigns, AccountGuard and Election Security Advisors to help monitor democracy in action.

> *"Disinformation comes in many forms, and no single technology will solve the challenge of helping people decipher what is true and accurate."*

Microsoft tackles the problem of deepfakes with Microsoft Video Authenticator. This program analyzes photos and videos and provides a "confidence score" indicating whether the media has been manipulated. The software detects the "blending boundary" along with "subtle fading or greyscale elements" that human eyes typically cannot see. Video Authenticator uses a public data set from "Face Forensics++," and was tested with the "Deepfake Detection Challenge Dataset."

As deepfakes become increasingly sophisticated, new detection methods must be devised. Few such tools exist today. Microsoft technology built in partnership with the Defending Democracy Program will help to power Project Origin.

Multiple technologies to detect disinformation campaigns must be widely adopted, and consumers must be educated about them.

Microsoft, partnering with the AI Foundation, a nonprofit San Francisco company, supports the global spread of AI technology. Project Origin will test AI authenticity through a consortium of media organizations. The Trusted News Initiative encourages content publishers and social media entities to work together to combat disinformation. Media literacy programs help people sort facts from disinformation and to identify deepfakes.

> *"Practical media knowledge can enable us all to think critically about the context of media and become more engaged citizens while still appreciating satire and parody."*

Microsoft's "Spot the Deepfake Quiz" is being launched as an interactive media literacy tool in partnership with the University of Washington Center for an Informed Public, Sensity, and *USA Today*. Microsoft also created a public relations campaign encouraging the public to take a closer look at the media they consume. Its program "NewsGuard" asks professional journalists to rate websites based on integrity. The service can be downloaded using any standard browser.

Did you like this summary?

Read the article

https://getab.li/44145

This document is restricted to personal use only.

getAbstract maintains complete editorial responsibility for all parts of this abstract. All rights reserved. No part of this abstract may be reproduced or transmitted or used for training any machine learning system in any form or by any means – electronic, photocopying or otherwise – without prior written permission of getAbstract AG (Switzerland).