Analysis of privacy data for users of online services

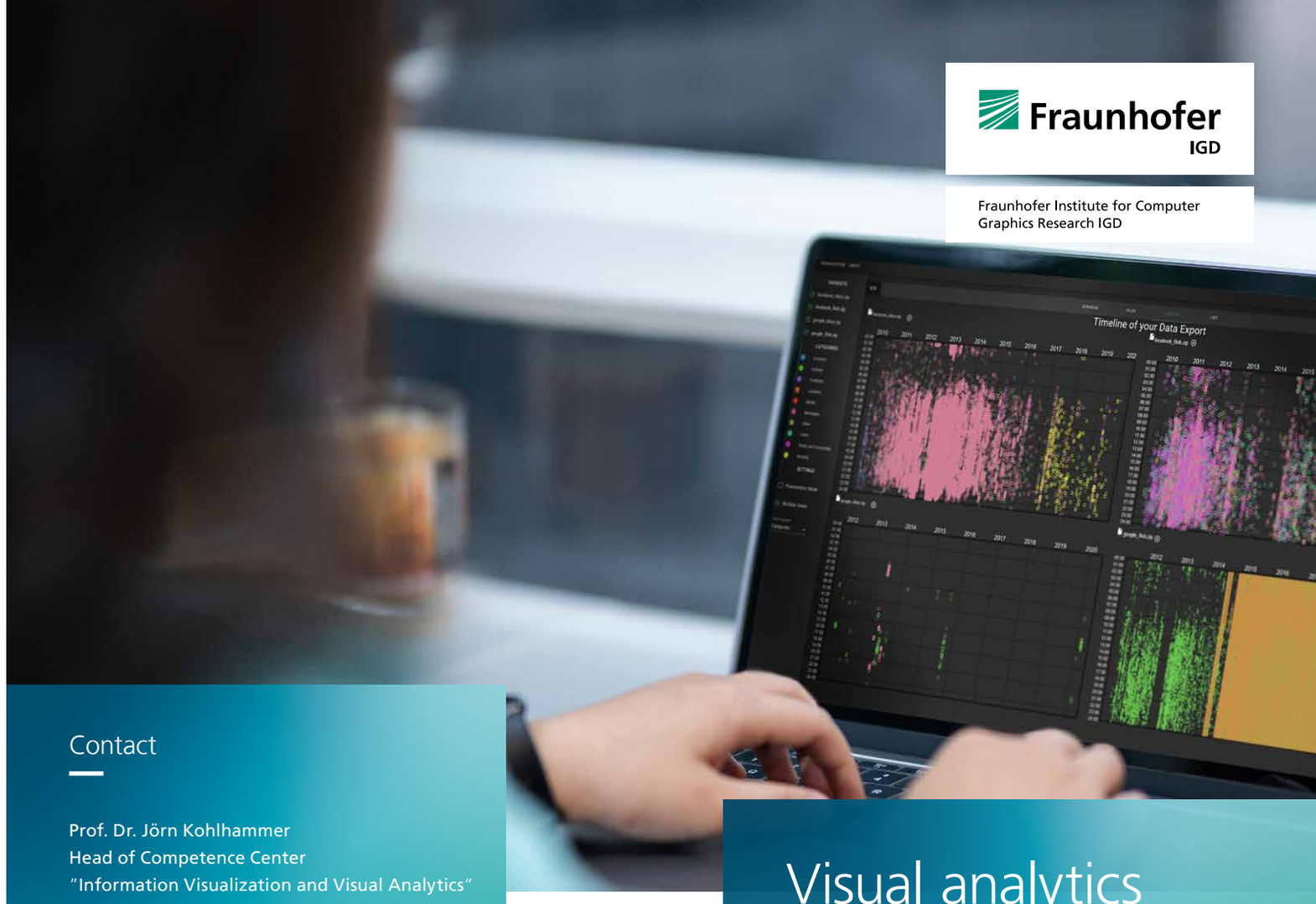
Online services are used for a variety of activities such as messaging, conversations or content sharing. These possibilities create a range of new privacy threats—e.g. due to facilitation of surveillance or through databases with personal data. In most cases, users have relatively little overview over their personal data which are collected during their usage of online services. With our TransparencyVis technology, users can explore their GDPR downloads from many online services and gain such an overview.

Try it out with your own data:
https://transparency-vis.vx.igd.fraunhofer.de

Visual Analysis of Software Vulnerabilities

Today's software systems are created in complex software development processes that naturally induce mistakes, some of which can be exploited by attackers and are therefore called vulnerabilities. Automatic software scanners enable developers to analyze their applications to detect, verify and resolve vulnerabilities. Our interactive visualization further supports developers and security experts in gaining an overview of the security state of their application and to prioritize the correction of vulnerabilities.

Our team has proven expertise in user studies, consulting and development projects in the area of visualization and visual analytics for cybersecurity and privacy. Our visualization solutions combine specific users' needs, data and tasks to create a specific customer solution. We provide our skills in applied research, applying the principles of user-centered design.
Contact us to learn more.



Fraunhofer IGD

Fraunhofer Institute for Computer Graphics Research IGD

Visual analytics for cybersecurity and privacy

Contact

Prof. Dr. Jörn Kohlhammer
Head of Competence Center
"Information Visualization and Visual Analytics"
Phone: +49 6151 155-646
joern.kohlhammer@igd.fraunhofer.de

Fraunhofer Institute for Computer Graphics Research IGD
Fraunhoferstr. 5
64283 Darmstadt, Germany

www.fh-igd.de/cybersecurity

V04-22-01

ATHENE
National Research Center for Applied Cybersecurity

Visual analytics for cybersecurity and privacy

Cyberattacks typically target weaknesses within the Internet, causing disruptions to reliable operation and endangering the integrity of services and organizations that rely on it. **Interactive forensics** play a key role when analyzing new, unknown vulnerabilities. This requires large volumes of data to be processed and visualized. In this context, visual analytics methods have proven effective, as they **combine automatic data analytics algorithms with new visualization methods**, thereby allowing experts to interact with this data.

ATHENE – National Research Center for Applied Cybersecurity

As a partner in ATHENE, the National Research Center for Applied Cybersecurity in Darmstadt, Fraunhofer IGD researches and develops solutions, strategies and technologies for the **visualization** of decision-relevant data in cybersecurity and privacy protection. Fraunhofer IGD's Competence Center of Information Visualization and Visual Analytics focuses on the following areas:

- Visual and interactive analysis of network data
- Visualization of global Geo-IP routes
- Analysis of privacy data for users of online services
- Visual analysis of software vulnerabilities

Visual and interactive analysis of network data

The analysis of network data is highly relevant for network administrators and security experts. Such data typically has to be laboriously analyzed with tools such as Wireshark. Our technology NetCapVis allows the visual and interactive analysis of this data for a more effective and faster workflow. It allows interactive working with massive PCAP data, while providing the means for effectively identifying anomalies supported by AI methods.

Try it out yourself at:
https://netcapvis.igd.fraunhofer.de

Visualization of global Geo-IP routes

When assessing network connections, it is useful to leverage geographic information. Currently, there are only online services that indicate the current location for a specific IP address. Our proBGP technology makes it possible to identify and visualize an IP block and follow its changes over time. Moreover, the routing between IP blocks can be analyzed to detect anomalous diversions from typical routes.

Our web prototype is accessible at:
https://probgp.igd.fraunhofer.de