# Kurzfassung

Durch die Nutzung allgegenwärtiger digitaler Anwendungen, die heutzutage für verschiedene alltägliche Zwecke nahezu unabdingbar sind, hinterlassen Nutzer:innen unzählige Spuren persönlicher Daten in diesen Anwendungen und im Internet. In dieser Arbeit wird untersucht, welche Arten von Informationen in verschiedenen Anwendungsfällen, die Millionen von Nutzer:innen täglich betreffen, preisgegeben werden. Dies umfasst sowohl Informationen, die aktiv anderen Menschen zur Verfügung gestellt werden, z.B. durch das Teilen von Inhalten in sozialen Netzwerken, als auch Informationen, die allein durch die Nutzung bestimmter Anwendungen, z.B. mobile Messenger, offenbart und von anderen erlangt werden können, auch wenn es von den entsprechenden Nutzer:innen nicht beabsichtigt ist.

Hinsichtlich aktiv geteilter Informationen ist das Langzeitmanagement der Informationsverfügbarkeit ein wichtiger Anwendungsfall, im Besonderen das kontrollierte Vergessen von Daten unter bestimmten Bedingungen. In diesem Zusammenhang wird eine umfassende Systematisierung existierender Forschungsarbeiten zum Thema Langzeitmanagement von Online-Daten durchgeführt. Dabei werden verfügbare technische Konzep-te zur Reduzierung der Sichtbarkeit den Erkenntnissen aus Nutzerstudien zum Umgang mit Online-Daten gegenübergestellt und Forschungslücken zwischen beiden Seiten identifiziert und analysiert. Akademische Konzepte für den Verfall von Daten, die zwar technisch Sicherheit garantieren, spiegeln die Bedürfnisse von Nutzer:innen im Hinblick auf den Umgang mit ihren Daten aber nicht angemessen wider. Deshalb wird ein fundamental anderer Ansatz vorgeschlagen, der verschiedene Perspektiven, unter anderem juristische Aspekte, mit einbezieht und mit dem Nutzer:innen und Online-Dienste das Ende der Verfügbarkeit von Online-Daten mithilfe von Smart Contracts vertraglich festlegen können. Derartige Vereinbaren ermöglichen eine flexiblere Spezifizierung des Man-

agements der Daten, und können auch so eingesetzt werden, dass für den Online-Dienst ein Anreiz geschaffen wird, den Verfall der Daten zu realisieren.

Im Gegensatz zum aktiven Teilen von Daten erlaubt auch die reine Nutzung bestimmter Online-Anwendungen, dass Außenstehende Informationen über Nutzer:innen gewinnen können. Der Anonymisierungsdienst Tor erlaubt, die eigene Identität bei der Nutzung des Internets zu verschleiern. Durch die Analyse von Netzwerkverkehr können die Aktivitäten von Nutzer:innen prinzipiell jedoch wieder nachvollzogen werden, was unter kontrollierbaren Rahmenbedingungen sehr gut funktioniert. In diesem Kontext wird untersucht, wie realistisch derartige Deanonymisierungsangriffe unter Berücksichtigung der echten Netzwerkinfrastruktur sind. Weiterhin wird im Fall von mobilen Messengern analysiert, in welchem Ausmaß Nutzer:innen von ihren Kontakten über einen unerwarteten auf Zeiten basierenden Seitenkanalangriff überwacht werden können. Die Zeit, die vergeht, bis eine gesendete Nachricht auf dem Sendegerät als zugestellt bestätigt wird, unterscheidet sich zwischen verschiedenen alltäglichen Orten aufgrund der Eigenschaften unterschiedlicher Internetanbindungen. Das Beobachten solcher unterscheidbarer Zeiten ermöglicht daher, allein durch das Senden von Nachrichten, den aktuellen Aufenthaltsort eines Empfangsgeräts zu bestimmen.