OFFICE OF FINANCIAL RESEARCH
U.S. DEPARTMENT OF THE TREASURY

Office of Financial Research
Working Paper #0011
September 4, 2013

Cryptography and the Economics of Supervisory Information: Balancing Transparency and Confidentiality

Mark Flood,[1] Jonathan Katz,[2] Stephen Ong,[3]
and Adam Smith[4]

[1] Office of Financial Research, mark.flood@treasury.gov
[2] University of Maryland, jkatz@cs.umd.edu
[3] Federal Reserve Bank of Cleveland, stephen.j.ong@clev.frb.org
[4] Pennsylvania State University and Office of Financial Research, asmith@cse.psu.edu

Cryptography and the Economics of Supervisory Information: Balancing Transparency and Confidentiality

Mark Flood[*] Jonathan Katz[†] Stephen Ong[‡] Adam Smith[*,§]

September 4, 2013

Abstract

We elucidate the tradeoffs between transparency and confidentiality in the context of financial regulation. The structure of information in financial contexts creates incentives with a pervasive effect on financial institutions and their relationships. This includes supervisory institutions, which must balance the opposing forces of confidentiality and transparency that arise from their examination and disclosure duties. Prudential supervision can expose confidential information to examiners who have a duty to protect it. Disclosure policies work to reduce information asymmetries, empowering investors and fostering market discipline. The resulting confidentiality/transparency dichotomy tends to push supervisory information policies to one extreme or the other. We argue that there are important intermediate cases in which limited information sharing would be welfare-improving, and that this can be achieved with careful use of new techniques from the fields of secure computation and statistical data privacy. We provide a broad overview of these new technologies. We also describe three specific usage scenarios where such beneficial solutions might be implemented.

The authors gratefully acknowledge helpful comments from and discussion with Peter Bloniarz, Jill Cetina, Greg Duffee, Greg Feldberg, Benjamin Kay, Matt McCormick, Claudio Orlandi, Mallesh Pai, Bill Treacy, and Valerie Wells, as well as participants at research workshops at Penn State's Center for Financial Stability (March 2012), the Office of Financial Research (April 2013), the California Institute of Technology (May 2013), and the Federal Reserve (May 2013). Any remaining errors or omissions are the responsibility of the authors alone.

Adam Smith's work at Penn State was supported in part by National Science Foundation awards #0941553 and #0747294. Jonathan Katz's work was supported in part by National Science Foundation award #1111599.

Views and opinions expressed are those of the authors and do not necessarily represent official OFR or Treasury positions or policy. The views stated herein are those of the authors and are not necessarily those of the Federal Reserve Bank of Cleveland or of the Board of Governors of the Federal Reserve System.

Comments and suggestions are welcome and should be directed to the authors.

[*]Office of Financial Research, U.S. Department of the Treasury, Washington, D.C.

[†]Computer Science Department, University of Maryland, College Park, Md.

[‡]Federal Reserve Bank of Cleveland, Cleveland, Ohio

[§]Computer Science and Engineering Department, Pennsylvania State University, University Park, Pa.

Contents

1 The Transparency-Confidentiality Tradeoff

This paper has several goals: First, we elucidate the tradeoffs between transparency and confidentiality in the context of financial supervision. Second, we explore how developments in cryptography, statistical data privacy, and secure computation provide conceptual tools to formulate confidentiality requirements precisely, and technologies to enforce them, while still revealing useful information (see Section 4 for definitions of technical terms). Our main thesis is that a careful application of these new techniques can alleviate some of the tension between transparency and confidentiality in important practical cases for financial regulators. Finally, we identify directions for future research necessary to make these tools more applicable to the context of financial regulation.

There is a natural tension between transparency and confidentiality inherent in financial activity. Excessive or uneven disclosure can discourage financial activity, but well-chosen summary statistics can serve as public goods if widely disseminated.[1] For example, although market-makers and others intentionally conceal individual transaction amounts and portfolio positions to protect proprietary strategies or avoid trading losses, transaction prices in most markets are widely available to help guide investment decisions toward an optimal aggregate allocation of capital.

We begin with the premise that regulators can assist in this context by requiring the standardization and dissemination of information to improve decision-making in the aggregate. The challenge is in calibrating policies to maximize transparency as a public good, while respecting existing institutions and commitments, enforcing laws and regulations, and minimizing the potential for damaging side effects on financial activity, supervisory relationships, and financial innovation. Finding a suitable balance among the competing objectives of financial firms, their customers, supervisory agencies, and the general public thus requires a careful configuration of rules, processes, and technologies. Either excessive transparency or excessive confidentiality can be harmful, depending on the particular situation. As Fung et al. [83] emphasize in their recent survey, the implementation details of transparency policies matter by making a difference in how data are collected and presented, in addition to the question of what information is shared, and with whom. This paper discusses processes and technologies for reducing information asymmetries across organizational boundaries, focusing on regulator-mandated disclosures, especially those resulting in formally restricted supervisory information. There is a devil in the details, both in identifying the goals for information sharing, as well as for crafting processes and choosing technologies to assist in the implementation.

To illustrate the potential (and limitations) of the new technologies in a supervisory context, we propose three specific case studies:

- Publication of Aggregated Sensitive Data: Financial regulators, including a number of Federal Reserve Banks, have recently introduced public indexes of financial conditions; see Office of Financial Research [169, pp. 38-45]; Oet et al. [168]. These measures condense a complex financial system into single numbers that can be tracked through time. Because these signals can affect significant financial decisions, there are costs or losses associated with both false positives and false negatives. In some cases, expanding the set of data inputs for the index calculation can improve the accuracy of the index; see Oet et al. [166]. Unfortunately, these enhancements can be blocked by legal restrictions due to licensing agreements, privacy laws, and confidentiality of supervisory data. However, it may be possible to design cryptographic implementations to "sanitize" the signal, such that we can guarantee that it is impossible (within specific tolerances) to reverse-engineer the confidential inputs from the published index.
- Retail Loan Information to Support Research: Regulators have begun to collect highly granular datasets on retail loan exposures, including home mortgages and credit cards; e.g., Consumer Financial Protection Bureau [40], Qi [177]. There is a significant research component to the work that these agencies are performing; the datasets contain millions of records of granular detail on financial relationships and behavior. Supervisory analysis would benefit greatly if the data could be shared

[1] Specifically, a published signal is a public good if it is both non-rivalrous (my "consuming" the signal does not leave any less of it for you) and non-excludable (the act of publication implies that access is unlimited).

with the broader research community, but this is not immediately possible due to privacy restrictions. However, only the aggregate patterns are typically of interest to financial researchers, rather than borrower-level details. It may be possible to randomize the data in ways that preserve aggregate patterns, while disguising individual details, and to use techniques of differential privacy to calculate the corresponding guarantees and tolerances.

- International Sharing: The recent financial crisis was an impetus to expanded international regulatory data sharing, exemplified by the Data Gaps Initiative of the Group of Twenty (G-20) ([74], [77]). Some of these recommendations consider sharing data about individual institutions with international supervisory colleges, including Recommendation #8 on sharing data on linkages between individual firms, and Recommendation #9 to create a common template for data reporting. These recommendations recognize that sharing introduces important confidentiality concerns. One obvious concern is the limited cross-border authority and jurisdiction to govern disputes and misunderstandings once the data have left home. Techniques of secure multiparty computation may allow for international signals and statistics to be calculated in a distributed fashion so that the underlying granular data never need to be centralized or shared.[2]

We emphasize that the new computational techniques, although useful, are not a panacea. They are practical technologies with the potential to improve outcomes in particular cases. Successful implementation requires careful consideration of the details of: (a) "Who are the parties involved in sharing?" (b) "What is to be computed—or what information should be shared?" and (c) "What is to be protected—or what should not be shared?"

The paper proceeds in four sections. The next section reviews the literature on the economics of information for general lessons on the potential benefits and pitfalls of transparency. We pay special attention to financial disclosure policies and information asymmetries in the financial sector. Section 3 examines the particular experience of financial regulators with information sharing, and the various confidentiality and privacy concerns that have arisen. Section 4 reviews potentially relevant tools and concepts from the fields of cryptography and statistical data privacy for a better understanding of how those technologies might be applied, and what further research is necessary, in the specific context of financial supervision. We close in Section 5 with three illustrative proposals for possible applications of the tools to concrete supervisory challenges.

The general conclusion is that information sharing among financial regulators and transparency to the broader public can produce significant concrete benefits. Techniques for secure computation can assist in this process by reliably filtering the information that should and should not be disclosed. This filtration represents a middle ground between the traditional choice of full publication and full confidentiality.

2 Costs and Benefits of Full Transparency

Most discussions of supervisory disclosure assume a choice between the two extremes: regulators will either keep information tightly confidential or make it fully public. This stark dichotomy is due in part to difficulties supervisors face in guaranteeing that sharing of data will be "limited," coupled with an asymmetric loss function (for both firms and regulators) that assigns extra weight to favoritism or inequity in disclosure. For example, the General Accounting Office [90, p. 21] identifies as an obstacle to practical data sharing among regulators the potential for liability in the case of disclosure of sensitive regulatory information, personally identifiable information (PII), and unverified prejudicial information, such as consumer complaints.

At the same time, there may be social-welfare benefits from additional supervisory disclosures or data sharing. Publication of signals that reduce information asymmetries (while protecting vital trade secrets of individual participants) may improve the allocation of risks and investible capital. By all accounts, more extensive sharing among the relevant financial regulators would have improved overall situational awareness

[2]These techniques are highlighted in a recent paper by Abbe et al. [1].

and policy responsiveness in the crucible of the Lehman crisis in 2008.[3] More speculatively, publication of the daily aggregate open interest in the over-the-counter market (OTC) for credit default swaps (CDSs) might have motivated market discipline to deflate the subprime securitization bubble sooner than the "run on the repo" in August 2007.[4] Both of these examples—exposing aggregates while concealing firm-specific details, and sharing facts or calculations among a limited set of privileged policymakers—represent a middle ground between fully public disclosures and closely guarded supervisory secrets. The case studies introduced above and discussed below (Section 5) are similarly intended to negotiate these intermediate possibilities, by applying promising new techniques from the field of computational privacy. On the other hand, we emphasize that additional transparency is not automatically beneficial; welfare-enhancing disclosures require careful consideration of what is revealed to whom, and under what conditions.

2.1 Asymmetric Information and Disclosure Regulations

The informational and governance "terrain" of financial markets differs from that of intermediary firms. Markets commit financial resources and risk-bearing capacity in contractual relationships between participants; intermediaries localize financial decisions within the firms themselves. The primary transparency channel in most financial markets is the post-trade transparency of transaction prices. In contrast, financial firms are circumscribed by legal, commercial, and technical boundaries, and financial commitments are managed by internal governance processes. The primary transparency vehicle for individual firms is the publication of standard quarterly or annual accounting statements. This institutional context matters for regulatory disclosure, because the primary regulators for various industry segments are limited by different legislative mandates and constraints, as well as the accumulated precedent of rulemakings and guidance.

A tenet of the industrial organization literature is that, over the long term, institutional structures and information structures are jointly and endogenously determined. The locus of financial activity—within firms versus between firms—depends on transaction costs and information problems. In particular, information asymmetries, agency problems, and other knowledge gaps, such as unforeseeable contingencies, imply that contracts cannot be complete. By construction, arm's-length transactions create idiosyncratic information sets, which tend naturally to diverge across participants. Such imperfections can provoke enforcement disputes and ex-post bargaining problems that discourage contracting. In Akerlof's seminal model [4] of adverse selection, only "lemons" are offered in the used-car market because sellers cannot credibly warrant a vehicle's true accident history and mechanical reliability without a costly inspection. At the extreme, the danger of adverse selection drives away transactions altogether: in the no-trade theorem of Milgrom and Stokey [153], a Pareto-efficient starting allocation implies that any offer to trade at the ex-ante equilibrium price must be evidence of asymmetric information, which a risk-averse counterparty should therefore refuse. Roughly re-stated, if everyone knows that the only motivation for trading is to pursue a buy-low/sell-high strategy—e.g., to exploit counterparties by underpaying for assets—then no one will enter the market at all.

In contrast to financial markets, intermediary firms internalize decisions to allocate financial resources. Only the "last-mile" interactions with end users such as depositors and borrowers involve formal contractual commitments, while the broader portfolio allocation decisions are internalized. This approach facilitates the

[3] The Financial Crisis Inquiry Commission [72, p. 329] states that, "regulators did not know nearly enough about over-the-counter derivatives activities at Lehman and other investment banks, which were major OTC derivatives dealers." In her testimony to the House Financial Services Committee in April 2010, Chairman Schapiro of the Securities and Exchange Commission (SEC) cited four major initiatives the SEC was undertaking in response to the Lehman failure, three of which focus on improving information systems and sharing: (a) improvements to broker-dealer reporting and monitoring; (b) improved coordination. (i.e., "full information sharing"); (c) improved examination, oversight and enforcement; and (d) further improvements to rules and requirements; [183].

[4] Although it does not speculate on the counterfactual possibility of publishing CDS market aggregates before the crisis, the Financial Crisis Inquiry Commission [72, p. 352] concludes that, "The OTC derivatives market's lack of transparency and of effective price discovery exacerbated the collateral disputes of AIG and Goldman Sachs and similar disputes between other derivatives counterparties. AIG engaged in regulatory arbitrage by setting up a major business in this unregulated product, locating much of the business in London, and selecting a weak federal regulator, the Office of Thrift Supervision (OTS)."

responsiveness of portfolio management by avoiding costly re-contracting ([203], [191]), but the efficiencies of integrating services and decisions within a financial intermediary must be traded off against the efficiencies of specialized providers and the concomitant costs of transacting. Over time, the balance point has shifted as innovations in derivatives valuation have vastly expanded the markets for hedging instruments, reducing the hazard of ex-post re-contracting for many transactions. The decrease in contracting costs has been compounded by a general drop in the cost of managing information, as advances in electronic messaging, computation, and storage have increased the operational capacity for transaction flows. The long-run trend reveals a clear and steady shift away from intermediated activity and into the transacted sector. The upshot is a significant increase in data and information to be structured, stored, and shared among market participants, in the form of quotes, transaction confirmations, contractual details, payment messages, etc. This trend implies a general shift to market prices and away from internal firm governance as a coordination mechanism for financial activity.

From a supervisory perspective, this shift implies new data-collection and sharing challenges. The migration into new markets will typically reduce supervisory scrutiny; much of the recent growth occurred in "shadow" banking sectors that do not fit neatly into traditional monitoring routines. The activities creating the greatest incentives for such regulatory arbitrage are likely those that should most concern supervisors. There is a long-standing debate regarding parochial competition in laxity between regulators.[5] Regardless of whether supervisors consciously pursue such competition, interagency coordination, including data sharing, should reduce incentives for "forum shopping" by entities seeking to evade regulatory interference.

In theory, the transparency of prices typical of financial markets should ultimately resolve most asymmetries: the efficient markets hypothesis (EMH, [68]) asserts that observed prices will "fully reflect" all available information, while the First Welfare Theorem asserts that equilibrium under complete Arrow-Debreu markets will be Pareto-optimal [87]. If both assertions were always true, questions of information sharing would be largely moot. Indeed, Feldman and Schmidt [71, p. 7–8] point out that market prices have some advantages even over supervisors' traditional access to the full internal books and records of banks, including the fact that prices are timely, forward-looking, and aggregate the perspectives of numerous participants with financial incentives for accuracy; they argue that regulators can leverage these characteristics to induce market discipline of regulated institutions. Securities regulators have similarly leveraged rating agencies to add transparency to securities exposed to credit risk.

Unfortunately, both the EMH and the assumptions of complete markets are violated in a variety of significant and well known ways, with the upshot that prices alone are inadequate for eliminating information asymmetries. Most basically, prices are a direct measure of activity in financial markets, but only an indirect measure of activity within financial firms. For example, the Merton [150] model implies that equity values should be increasing in both the mean and volatility of asset returns, so that stock prices can be an ambiguous signal of bank asset quality, especially as leverage increases. The corporate veil is informational as well as legal, and can create opaqueness around financial activities and exposures. Fama [67, 409-410] concedes that the strong form of the EMH is prima facie dubious. This opacity can have consequences. Dang et al. [45] and Gorton [97] argue that extreme asymmetries—whether real or perceived—can drive the widespread exit from markets for opaque securities. We emphasize that asymmetry alone can be problematic, separate from any determination of actual portfolio quality. Peristiani et al. [173] note that publication of supervisory stress test results in 2009 helped alleviate a significant asymmetry caused by the opacity of large bank asset portfolios; the intensity of the crisis began to abate in the wake of that announcement.

Second, because information is costly to acquire, the learning process induces an equilibrium level of inaccuracy in prices. The anticipated trading profits due to informational advantages are a powerful motivator for research that increases the aggregate level of knowledge over time [100]. For example, search costs can overwhelm the arbitrage mechanism, even for very straightforward comparisons. Hortaçsu and Syverson [109] and Elton et al. [63] show empirically that seemingly identical S&P 500 index mutual funds exhibit a wide range of fees. Theoretically, the economic rents enabled by search frictions lead to overentry and excessive diversity in product markets [6]. At the individual level, they lead to adverse selection gains

[5]For example, Meyer [151, p. 21] states, "Nothing could be more disastrous than competition between the State and national banking groups based upon competition in laxity."

and losses. In the context of regulatory transparency policies, Fung et al. [83, ch. 4] emphasize the crucial practical importance of the comprehensibility of disclosures and their compatibility with decision-making: disclosed information should be readily available to end users at the right place and the right time. Even when search is successful, learning can take time, creating temporary divergences between current prices and the efficient ideal [134].

Third, markets may be incomplete in the sense that there are not enough prices to form sufficient statistic for all of the informational dimensions of interest. By construction, the migration of financial activity from intermediaries to markets creates traded prices where they did not exist before. Those new prices are either redundant or informative, suggesting again that the system operates at an informational margin and that there are always some dimensions of interest that the price vector is not capturing. More significantly, certain key dimensions defy measurement even after a problem has been clearly identified. These Knightian uncertainties include complexity ([42], [7]) and regime shifts [36].

2.2 Fine-tuning Information Disclosure

If firms are opaque and the market prices of their equity and liabilities provide imperfect signals, one obvious solution is simply to publish more facts. Following Justice Brandeis's dictum, "sunlight is said to be the best of disinfectants; electric light the most efficient policeman," [34, p. 92] the Securities and Exchange Commission (SEC) initiated public disclosure of standard accounting reports under the Securities Acts of 1933 and 1934 to reduce informational asymmetries in the markets. Fung et al. [83, p. 39] highlight SEC disclosure as a successful example of so-called "targeted transparency" policies, which are characterized by a clearly specified: (1) policy purpose, (2) discloser population, (3) scope of information, (4) reporting vehicle, and (5) enforcement mechanism. While the SEC's disclosure rules focus on publicly traded firms, regulatory disclosure of financial statements for financial intermediaries is much broader: bank Call Reports, Thrift Financial Reports (TFRs, discontinued in March, 2012), and bank holding company (BHC) Y-9 reports cover the vast majority of depository institutions, including firms that are not publicly traded. For national banks, annual public reporting, via the Office of the Comptroller of the Currency (OCC), of basic, standardized accounting statements goes back to the National Bank Act in 1863. Despite all of this public disclosure, the challenges of opacity and incentives for moral hazard in banking remain.

Both the feasibility and desirability of full transparency are more nuanced in reality. At the most basic level, firms may simply not comply with disclosure rules, as evidenced by the Enron case [17]. Assuming effective compliance, practical trade-offs still exist, and the reality of disclosure practice typically occupies the middle ground. SEC disclosure regulations identify a finite set of standard public reports, while recognizing the need for disclosers to maintain a private set of trade secrets, strategic plans, and other confidential information. Under 240.10b-5 of the Securities Act of 1934 and Regulation FD (Fair Disclosure, [185]) the focus is on symmetric disclosure. For example, FD prohibits selective sharing of material nonpublic information as tantamount to illegal insider trading. "Public broadcast" addresses cross-sectional asymmetries, but leaves room for certain forms of intertemporal discretion in information release. For example, Kothari et al. [131] show that, on average, managers tend to delay the release of bad news compared to good news. Especially notable are the formal mechanisms by which investors intentionally ignore information. For example, to help in navigating conflicts, the SEC has created "trading plan" and "blind trust" exemptions to Rule 10b5-1 that allow investors to pre-commit to auditable processes that exclude information from investment decisions [186].

As with corporate disclosure, the practicalities of information sharing in financial markets are intricate. There can be significant trade-offs between liquidity and transparency, and institutional compromises have emerged to balance them. For example, many markets provide for the routing of quotes and orders through brokers to provide anonymity to the counterparties to protect against adverse selection. Payne [172, p. 316] describes the trade-off in the context of the spot foreign exchange market:

> ... discussion should focus on the implications of differences between electronically brokered trading and direct trading ... The former offers trading opportunities that are pre-trade anonymous but which are broadcast to the rest of the market. The latter offers trading opportunities

> that are nonanonymous but which remain private to the two counterparties. In our eyes, then, both avenues for trade have an advantage—the pre-trade anonymity of electronic brokers versus the post-trade opacity of direct trading.

Without protection from pre-trade transparency, dealers would often be less willing to take on large positions. Similar considerations are central to the development of so-called dark pool markets [114]. We emphasize, however, that heedless restrictions on pre-trade transparency will likely be counterproductive. Hendershott and Jones [105] cite the natural experiment of the Island electronic communication network (ECN), which in 2002 chose to "unpublish" its automated limit order book in response to new SEC rules under Regulation ATS (Automated Trading Systems). The result of this blanket moratorium on pre-trade transparency was a marked reduction in price discovery and market share for the Island ECN, together with an increase in trading costs.

Conversely, Boehmer et al. [29] find that publication of the full limit-order book at the New York Stock Exchange (NYSE), introduced as "NYSE OpenBook" in 2002, reduced the advantages of the NYSE specialists and improved market liquidity. Bessembinder et al. [19] find similar evidence of liquidity improvements in the OTC market for corporate bonds following introduction of the SEC-mandated Trade Reporting and Compliance Engine (TRACE) in 2002. TRACE boosts post-trade transparency by requiring publication of transaction details within 15 minutes. These improvements include a "liquidity externality" that spills over to markets for non-TRACE-eligible bonds. Reductions in rent extraction in bond markets may simply have pushed informed traders over into the closely related CDS market, however. Avellaneda and Cont [8] argue that large CDS dealers are especially vulnerable to information asymmetries; as long as the system relies on their inventory capacity as the primary buffer for aggregate liquidity, there should remain some "upstairs" venue protected from post-trade transparency.

Financial markets also produce cases in which information is intentionally discarded to reduce asymmetries. In the diamond markets, for example, the De Beers cartel uses its market power to enforce a set of discrete quality grades for diamonds [152], thereby truncating the private gains to bargain-hunting via minuscule sorting and grading of individual stones. Kenney and Klein [124] argue that this imposed constraint can add value, since "oversearching" might otherwise create a negative externality akin to Gresham's Law, driving away good diamonds like Akerlof's non-lemons. Holmström [107] sees a range of similar examples in the financial realm, including money market funds and money itself (both of which typically exchange at par), credit ratings, and tranched securitizations. This is essentially the same as the "generalization" method of bucketing to mask data via k-anonymity (see Section 4.2.4 below). In a financial context, the key is that the projection of the information set into a discrete set of quality categories can reduce asymmetries, so that private information becomes less relevant and overall market liquidity improves.

2.3 Information Sharing and Regulation

Information sharing is concerned with taking facts known to one party and making them also known to others, reducing information asymmetries in an obvious way. Social and strategic issues can cause the sum of individual informational sets to differ from the shared whole. For example, facts that are self-evident to individual participants can have different implications if those same facts are *common knowledge*. As in the parable of the emperor's new clothes, affirming publicly what each agent individually already knows to be true can alter behavior. The classic brain-teaser in this regard is the so-called Conway Paradox or "muddy faces" puzzle.[6] In these models, it is important to clarify: what is true; what is known individually by agent i to be true; and what agent i knows about what agent j knows to be true. An event is said to be *self-evident* to agent i if the truth of the event per se corresponds precisely to i's knowledge of the event. As a highly simplistic example, consider three events that might describe a particular bank: (1) prospering (or "investment grade"), (2) scraping by (or "junk"), and (3) in default. The fact (i.e., event) that the bank is

[6]The paradox has been retold repeatedly with a variety of settings, including muddy children, tactful ladies with smudged make-up, party hats of different colors, and cannibals with unfaithful wives. See Geanakoplos [86, 85] for an excellent introduction. For a good survey of models of asymmetric information in finance, including common knowledge issues, see Brunnermeier [35].

prospering may be self-evident to a supervisor who has just completed a full on-site examination and seen diligent accounting, competent managers, strong revenues and cash position, etc. On the other hand, a bank bondholder who knows only that coupon payments continue to arrive on time cannot distinguish between investment grade and junk; the true event (prospering) is not self-evident to her.

Knowledge becomes "common" when it is *mutually* self-evident: i.e., it is necessary that the participants individually know it, but also that everyone knows—recursively—that everyone else knows too. Another "paradox" illustrates how the transition from simultaneous knowledge to common knowledge can solve problems of coordinated action. In the "two generals problem," a pincer movement will succeed if both generals attack together, but if either army attacks alone it is doomed. Neither general is willing to act without absolute certainty of coordination, but they have no way to know for sure that their orders or acknowledgments are getting through to the other. Inductively, no accumulation of acknowledged acknowledgments can guarantee that the final messenger gets through. In the end, both are paralyzed by uncertainty of coordination: common knowledge—and therefore absolute certainty—is theoretically unachievable. The communications failure here is obviously partly due to the restrictive assumptions on messaging.[7]

These stylized examples have lessons for information sharing with and among regulators. For example, ratings agencies work to fill the information gap faced by bondholders without the resources to perform their own audit. Ratings can generate common knowledge by publicly announcing their ratings. However, in the noisy signal environment typical of financial markets, credibility of the signal is important. When the Federal Reserve announced the results of Supervisory Capital Assessment Program (SCAP) at the depths of the financial crisis in 2009, most market signals were highly suspect. The Fed's established credibility, combined with a highly visible stress-testing exercise, were critical in communicating common understanding and acceptance of bank solvency.[8] The economic notion of credible certification is closely related to the concept of a "trusted party" in secure multiparty computation, described below (Section 4.2) and reflected in the use cases on sensitive data (Section 5.1) and international sharing (Section 5.3). Regulators' lack of an immediate profit motive gives them an advantage in acting as a trusted or credible intermediary.

Nonetheless, an important threat to credibility is capture, the possibility that the signaling agencies will gradually align their behavior to benefit the firms they cover [133, 43, 118]. This threat drives a demand for costly signals and certification services, such as external audits, supervisory examinations, and warranties. Certifiers, in turn, invest in costly reputation-building, which can create natural monopolies for honest certification services [192]. As an alternative (or supplement) to trusted reporters, centralization of information can be critical to communication if it helps build common knowledge. The Financial Stability Oversight Council (FSOC) created by the Dodd-Frank Act works not merely by fostering bilateral channels between regulators, but by facilitating mutual communication, whereby facts and issues are aired in a plenary venue. The Office of Financial Research (OFR) is similarly tasked with centralizing information and standardizing it to facilitate interoperability and communication. On the other hand, Wagner [199] argues that agencies that fail to filter the inflow can be inundated with too much information, creating an alternate pathway to regulatory capture as supervisors turn to industry experts to help navigate the deluge. This information overload remains a long-run challenge for information sharing.

2.4 Lessons from the Economics of Information

This brief review of the economics of information, regulation, and disclosure yields five broad conclusions. First, the industrial organization of the financial services industry is intimately bound up with problems of information. Because the regulatory system is adapted to the institutional structure of firms and markets, the datasets available for sharing among individual regulatory agencies are idiosyncratic and constrained. Second, transparency can often create value by alleviating coordination problems. Financial information typically

[7] The problem is also known as "coordinated attack problem;" [65, 86]. The two-phase commit protocol of database theory resolves the pseudo-paradox by introducing a "commit coordinator" to centralize information, along with a willingness to continue messaging indefinitely until the commit occurs [99, p. 466].

[8] In contrast, when the rating agency S&P downgraded U.S. Treasury debt in 2011, Treasury yields actually dropped [193], implying that traders did not accept the prima facie interpretation of a credit downgrade. On the effectiveness of the SCAP, see also Pianalto [174].

exhibits the non-rival characteristic of a public good, and can be made non-excludable via publication; this suggests that we should expect it to be under-produced in a competitive equilibrium, and that there may be a role for welfare-enhancing intervention by regulators. Third, a primary channel by which information revelation enhances coordination is by reducing information asymmetries, which can enhance liquidity—or drive it out of markets in extreme cases. Fourth, successful disclosure regimes require careful attention to the particulars of the case: who is disclosing what to whom, and why. Simplistic "reveal everything" disclosures have the potential to backfire by discouraging market participation or overwhelming recipients with superfluous detail. Fifth, fully common knowledge can generate benefits beyond those created by simple symmetric information. In particular, information sharing among regulators should facilitate mutually beneficial coordination.

3 Relationships Involving the Sharing of Data

The fundamental tension described above (Section 2) between transparency and confidentiality has concrete practical manifestations in the form of laws, rules and policies. Financial supervisors rely heavily on information, including data proprietary to supervised firms. This reliance creates a need for confidentiality to preserve the reputation and competitiveness of the supervised firm and the integrity of the financial supervisor. At the same time, the economic and accountability benefits of disclosure create a need for openness. For example, Pianalto [174] argues that increased transparency of regulatory policy can aid coordination between regulated entities and their supervisors, while enhancing the credibility of the latter. Secrecy about regulatory plans can foster an atmosphere of policy uncertainty in which participants assume the worst and tensions of mutual distrust are reinforced. Note that the arguments presented in this paper in most cases do not require the presence of a central macroprudential authority; most of these techniques are available to individual microprudential supervisors.

3.1 Restricted Supervisory Information (RSI) and Data

In the U.S., the dominant tool in balancing the demands of transparency and confidentiality is the Freedom of Information Act (FOIA). The FOIA combines a presumption of disclosure with a set of nine specific exemptions that allow financial regulators (and other agencies) to maintain confidentiality when appropriate.[9] The exemption most relevant for financial supervision is 552(b)(8), which specifically exempts information "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions." [47].

The FOIA is only one of many federal laws that relate to the disclosure (or non-disclosure) of information between financial market participants, supervisors, and the public at large.[10] For example, the Privacy Act of 1974 and related legislation introduced a formal category of "personally identifiable information" (PII) with particular safeguarding requirements (Government Accountability Office [98]; McCallister et al. [144]). The Privacy Act protections were supplemented in 2002 with the passage of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA).[11] The CIPSEA designates three federal "statistical agencies" for special treatment: the Bureau of the Census, the Bureau of Labor Statistics, and the Bureau of Economic Analysis. The CIPSEA protects PII (and other information) collected by these agencies for

[9]The FOIA law appears at 5 USC 552, with the specific exemptions listed at 552(b); [91]. The White House recently re-emphasized the "presumption of disclosure" under FOIA in a memorandum to Executive Departments and Agencies ([202]), following a post-2001 slowdown in FOIA releases; [176].

[10]The legal and bureaucratic landscape is intricate; a non-comprehensive sampling of major laws appears in Appendix A. Moreover, each financial regulator implements its own rules, policies, and procedures to manage the interactions between the legislative rules and their practical information challenges. The upshot is a complex array of largely regulator-specific rulesets for handling sensitive information. An agency-by-agency sampling of formal categories (see Appendix B) gives a sense of the scale and scope of the challenge.

[11]CIPSEA appears as Title V of the E-Government Act of 2002; see Appendix A; and Office of Management and Budget [170].

exclusively statistical purposes from unauthorized use, disclosure, or access, and permits them to share information with each other.[12] The CIPSEA and related guidance provide a valuable example of a coherent legal framework for collection, maintenance, sharing, and reporting of private information, including procedures for designating third-party collection "agents" and outside researchers who may handle the data. Although some of the CIPSEA provisions extend to "non-statistical agencies," such as financial supervisors, most do not.

The supervisory and statistical agencies responsible for publishing aggregate statistics and supporting scientific research have established procedures for disclosure control.[13] For example, in releasing the triennial Survey of Consumer Finances (SCF), based on detailed and voluntary household-level questionnaires on income and savings behavior, the Federal Reserve undertakes a formal disclosure review that includes, among other things, suppression (i.e., deletion) of key fields, data "blurring" (i.e., noise addition), and data bucketing.[14] As linkage attacks have become more sophisticated and linkable data more ubiquitous, the SCF disclosure reviews have tended to impose additional constraints; see, for example, Fries [82] and Kennickell and Lane [125] and the references therein. Another instructive example is census microdata. In managing disclosures, the U.S. Census Bureau (a CIPSEA statistical agency) empanels a Disclosure Review Board to approve published data "products." Formal procedures include rounding, noise addition, field suppression, synthetic data, and topcoding (i.e., rounding of extreme outliers to threshold percentile values); [208, 49, 197, 145]. Many of these techniques are also built into the Advanced Query System underlying the Bureau's online tool, "American FactFinder" [104]. As with the SCF, the increasing sophistication of linkage attacks has had an effect. For example, the Census Bureau no longer requests social security numbers as part of its Survey of Income and Program Participation, because respondents have gradually learned not to provide this datum [146].

Financial supervisors have a particular focus on confidential financial information collected from regulated entities through the supervisory process and formal reports. The various agencies use different terminology and frameworks to manage this information (see Appendix B). To avoid ambiguity, we coin a new umbrella term, "restricted supervisory information" (RSI), to encompass any financial supervisory data or information held by federal agencies and subject to any of these (or other) policies, rules, or laws that proscribe their disclosure to the general public.[15] Less formally, supervisors gather RSI directly from regulated firms. In a banking context, for example, this gathering includes financial data (account balances, investments, counterparty exposures, executive compensation, etc.) and nonfinancial information (minutes of board meetings, strategic plans, risk reports, incentive compensation terms, etc.). In addition, RSI from a bank examination often comprises information related to firms' customers. Loan and portfolio reviews might draw in customers' social security numbers and other PII, balance sheet and income information, and even business plans. Finally, supervisors themselves will also generate RSI, based on information gathered through the supervisory process (examination reports, financial analysis, assessments of firm management, and possible supervisory strategies, etc.). By design, this derived information provides important nonpublic insights into the firm.

Even within a supervisory agency, strong "need-to-know" rules typically restrict employees' access. For example, the Federal Reserve, with its multiple responsibilities for monetary policy, financial stability, and banking supervision, limits access to RSI to employees directly involved in the supervision. Legally, the RSI is property of the Federal Reserve. Upon employment, supervisory employees commit in writing to safeguard RSI, and breaches may result in employment termination. A separating employee continues to be restricted from sharing RSI post-separation. Beyond the immediate requirement to safeguard the financial

[12] Tuttle and Willimack [197, p. 14] point out that, "In the United States, which has a decentralized statistical system, confidential data cannot be shared across statistical agencies without legal authority."

[13] For a general overview of computational disclosure control, see Sweeney [194].

[14] The National Opinion Research Center (NORC) at the University of Chicago conducts the SCF on behalf of the Fed. Any NORC staff members who touch the data are legally bound (per a felony offense) to confidentiality throughout their lifetimes [159].

[15] For an itemization of regulations defining RSI, see Appendix B. In the following, we emphasize Federal Reserve CSI as a practical example of RSI, but most of the discussion should extend in a straightforward way to RSI in general, although the particulars of implementation will necessarily differ.

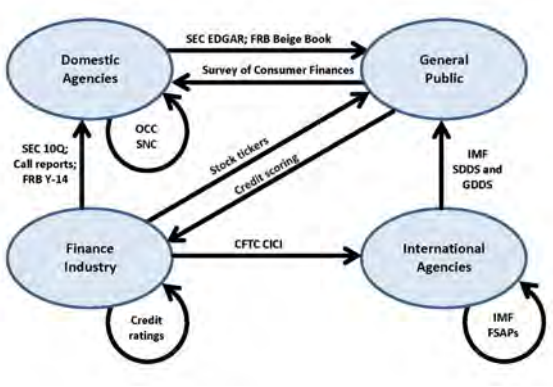

Figure 1: Some representative (non-comprehensive) examples of formal information-sharing among broadly defined financial user groups. The important role for transparency is reflected in the fact that the public receives information from all three other groups.

soundness and reputations of both participants and regulators (echoing the incentives for credibility described in Section 2.3), a primary goal of all of these restrictions is to foster a trusted relationship between firms and their supervisors, so that a reliable communications channel exists when it is most needed (foreshadowing the issue of trust, emphasized in Section 4.1).

3.2 Interagency Sharing of Information

Despite the many safeguards for RSI within particular supervisory agencies, there is frequently also a need to share information with other financial regulators. As the supervision and enforcement infrastructure has evolved over time, significant overlaps have emerged in the authority of the various supervisory agencies. For example, financial holding companies are a special class of large bank holding companies with diversified operations, and therefore multiple regulators, including potentially the full alphabet soup: Fed, Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency, SEC, and Commodity Futures Trading Commission (CFTC). Moreover, as emphasized above (Section 2.3), there can be important benefits to interagency coordination, a fact highlighted by the creation of the Federal Financial Institutions Examination Council in 1978, or more recently (2010) of the FSOC and OFR. To minimize regulatory burden, supervisors typically enter into memorandums of understanding to permit interagency information sharing. Generally, these agreements focus on agency-produced information, such as examination reports and review findings, which may include direct information regarding the supervised firm and its customers.

Figure 1 gives a sense of the scope of formal information-sharing among financial supervisors, industry participants, and the general public. The particular examples highlighted are far from a comprehensive listing. Indeed, just two of the many federal supervisors alone list scores of information collections for banks and bank holding companies [28]; and for public companies, investment advisors and broker-dealers [187]. Although current information-sharing channels are extensive, the effect of our use-cases would be to expand the repertory even further, from domestic supervisory agencies to the public (Section 5.1); from domestic agencies to the public and the research community (5.2); and from domestic to international agencies (5.3).

In addition to information sharing agreements, banking regulatory agencies have also entered into agreements, whereby representatives of the agencies jointly engage in the review of a particular aspect of the financial firm, or in the review of the financial firm overall. Information that is collected directly from the supervised firm is shared among the agency representatives who take part in the joint review. Although this information is shared among the participating supervisors, these supervisors may produce separate reports of examination and other agency-originated RSI, based on the information gathered directly from the supervised firm. In some instances, joint reports of examination and other supervisory memorandums are

produced by the agencies involved.

On the other hand, the rules can also work to complicate interagency coordination. The Gramm-Leach-Bliley Financial Modernization Act of 1999 required the Federal Reserve Board, "to the fullest extent possible," to defer to the examination reports of so-called "functional regulators" (e.g., the SEC) for non-depository subsidiaries of large financial holding companies [22, 26]. Although this deference might reduce the burden of duplicative examinations, it also creates a crucial dependency between supervisory agencies. The removal of the "second set of eyes" from direct inspection of the regulated entity magnified the need for interagency information sharing.[16]

In response to the financial crisis of 2007-08, Congress passed the Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) in 2010, with a key goal of promoting financial stability. As part of the Dodd-Frank Act, Congress created the FSOC to address the identified gaps in the entity-based supervision of financial firms.[17] In support of the FSOC, the Dodd-Frank Act also created the OFR under the Department of the Treasury. A key purpose for the OFR is to support the FSOC by collecting data on its behalf. The OFR has the authority to "share data and information ... with the Council [FSOC], member agencies, and the Bureau of Economic Analysis."[18] The responsibilities of the OFR Data Center include publication of certain reference databases, along with formats and standards for reporting data to the Office, while taking care not to publish any confidential data in the process. The OFR Data Center is also responsible to protect any data it collects against unauthorized disclosure.[19] In keeping with this mission and authority, the OFR strategic goals include providing "the public with key data and analysis, while protecting sensitive information" (Office of Financial Research [169, p. 127]). The OFR must balance the common-knowledge benefits (Section 2.3) of information accessibility against needs of information confidentiality—a balance not always easily achieved.

Given the global interconnectedness of large financial firms, the value of relevant, cross-industry financial information is international. Various initiatives are attempting to address this gap, such as the the Financial Stability Board's (FSB) Data Gaps Initiative ([77]) and the separate Enhanced Disclosure Task Force (EDTF) ([73]). The EDTF was charged with "improving the quality, comparability, and transparency of risk disclosures, while reducing redundant information and streamlining the process for bringing relevant disclosures to the market quickly." A unique aspect of the EDTF is the objective not merely to enhance the disclosure of raw data, but also the disclosure of business models, liquidity positions, and calculations of risk weightings of assets and other risk measures. The transparency goals of the EDTF are a good practical example of the pursuit of positive externalities through expanded disclosure, described in section 2. The public-good benefits are compounded as academics, researchers, nonprofit organizations, and others conduct research and analysis from varied perspectives. On the other hand, the potential for adversarial misuse of shared information—by competitive rivals, hackers, terrorists, etc.—looms larger in an international context. Our third use-case (Section 5.3) emphasizes this point, and suggests ways to use secure multiparty computation to balance the competing risks and benefits in this context.

3.3 Broadening Scope of Supervision

The historical evolution of bank examination provides an instructive example of the economic forces at work.[20] As noted above (Section 2.1), technological changes—especially the ability to structure contracts with a more complete specification of contingencies—have tended to encourage the migration of financial activity away from traditional intermediaries like banks. Many of those same changes have also tended to accelerate the pace of financial innovation, forcing a general move toward offsite monitoring and more

[16] Similar rules restricted the FDIC's ability to examine Federal Reserve member banks prior to 1950 [201, pp. 29–30].

[17] Dodd-Frank Act, section 112(a)(1).

[18] Dodd-Frank Act, section 153(b)(1).

[19] Dodd-Frank Act, section 154(b)(2).

[20] See White [201] for a more comprehensive history of bank examination in the U.S. Elliott et al. [62] consider the history of financial stability regulation. See Komai and Richardson [130] for a brief history of financial regulation more generally.

frequent examinations, including continuous on-site supervision for the largest firms. These trends have combined with more detailed and comprehensive reporting requirements to increase the overall volume of RSI to manage.

Reporting demands have grown yet again since the crisis of 2007-08. A central lesson from that episode was the potential for risk exposures in a large and innovative financial system to "shape-shift" and migrate in ways that may not be immediately apparent. The widespread shift of residential mortgages, including subprime loans, out of bank and thrift portfolios and into the "originate-and-sell" securitization chain moved large volumes of credit risk into new supervisory territory, with ramifications that were not fully understood.

Post-crisis reforms have sharply augmented the amount of RSI, as well as the mandate for interagency information sharing. A significant lesson embodied in the Dodd-Frank Act, for example through the creation FSOC and OFR, is that a strictly microprudential (entity-based) approach to supervision is not enough to ensure the stability of the financial system. Berner [18, p. 7] asserts that "we policymakers should ... make our first priority the expansion of data sharing among ourselves. The costs and obstacles are significant, but the benefits dwarf the impediments." Supervisors must also identify and monitor risk exposures shared among multiple firms or created by their interconnection and interaction. As a result, RSI from an individual firm may now also include information regarding its financial counterparties, increasing the volume and complexity of collecting and managing RSI.

4 Cryptographic Tools for Balancing Transparency and Confidentiality

In this section we describe two classes of cryptographic tools: *secure multiparty computation* (sometimes called secure function evaluation, SFE) and techniques for reasoning about and achieving *individual privacy in statistical data releases*. To understand what types of problems these tools address, it helps to recall some more familiar concepts from computer security. Public understanding of cryptography typically centers on the most widely-used cryptographic tools: encryption and signatures. Used correctly, these provide a *secure channel* between two parties, assuring each of them that messages received on the channel are authentic (they really come from the stated sender) and secret (no one except the intended recipient can learn anything about the message except perhaps its length). Secure channels are widely used and critical to storing, processing, and transmitting confidential information.

Secure channels are a tool for *access control*, which refers to a wide range of techniques for controlling the set of people or organizations able to read, modify, or distribute particular information. A relatively familiar example is the classification system for national security information [165]. Technologies to enforce access control and establish secure channels are not the focus of this survey. The manifold challenges facing any implementation of such technologies are not specific to the financial setting and are thoroughly covered elsewhere (see, e.g., [24, 95, 122] for textbook treatments). However, it helps to understand abstractly what these tools provide. They apply in settings where bright lines separate those who should be able to access specific data from those who should not. In contrast, the remainder of this section covers tools for reasoning about settings where no such bright lines can be drawn, and more subtle distinctions need to be made.

Over the past 25 years, the cryptography community has developed several tools that balance transparency and confidentiality. Both SFE and statistical data privacy stand out as relevant to financial data. These two classes of tools handle different types of concerns. Multiparty computation handles questions of how to release well defined output calculations without pooling input data in a single location; it effectively addresses questions of information *collection* and *storage*. In contrast, work on statistical privacy addresses questions of inferences that are possible based on released information (to the public or among regulators), possibly in combination with other sources of information.

The difference between these tools may be best understood through the metaphor of an incorruptible *trusted party*, to whom players can secretly send information and who will securely perform computations for them and reveal only the final results. Multiparty computation protocols emulate such a trusted party—for example, allowing regulatory agencies to compute aggregate statistics jointly without pooling data. In contrast, statistical privacy aims to understand and limit what confidential information is leaked by the

final output (aggregate statistics, for example). It is perhaps surprising that any information at all can be leaked by aggregate statistics, but it can; we discuss several examples in Section 4.2.3. Those examples also highlight problems with *personally identifiable information* (PII), which plays an unfortunately prominent role in current regulations.

Of course, the problem of protecting sensitive information is not new. Supervisors and statistical agencies have developed a number of robust techniques (see Section 3.1 for some examples). However, in some cases, recent research calls into question the appropriateness of current methodology. We describe multiparty computation and statistical privacy in Sections 4.1 and 4.2, respectively. Since the literature on the latter is largely specific to *individuals'* privacy, we discuss how it may be applied to financial privacy in Section 4.3.

4.1 Secure (Multi-Party) Computation

The standard technical tools for access control, previously mentioned, enforce binary, all-or-nothing information disclosure rules; an actor either has access to a particular document (or message), or does not.[21] However, many situations require the disclosure of information that can be derived from confidential data, while requiring that everything else about these data remain secret. In many such cases, access control tools are too coarse for the task.

To take a concrete example, consider the case of a one-sided or single auction. (The exact details of the goods, preferences, and auction mechanism are irrelevant for the current discussion.) We have a collection of bidders and a seller. The bidders all agree to the rules of the auction, and want to make sure that the auction is carried out correctly, e.g., the seller should not be able to preferentially choose one of the bidders to win the item (unless that bidder is the legitimate winner). The bidders may also be concerned about their privacy; they may not want to reveal anything about their bids to other bidders or even to the seller. Of course, some information leakage is unavoidable—the seller must learn the amount paid, and probably also the identity of the winning bidder. The bidders understand that this is inevitable, but don't want to leak anything *besides* this. We will return to this issue. The points to note here are (1) the setting is symmetric among the bidders, so it would be inappropriate to classify any of the bidders as being "good" or "bad"; rather, each bidder can be viewed as having interests in opposition to those of the other bidders, and (2) even if there is complete trust that all parties will run the auction honestly, bidders might still prefer their bids to be kept private lest that information be used to their disadvantage in future auctions or negotiations.

4.1.1 Trusted Parties and the Ideal/Real Paradigm

In considering complex scenarios, it helps to imagine an ideal in which the players all agree on an incorruptible "trusted party." This party is trusted to (1) carry out any desired computation correctly, and (2) maintain confidentiality of any data it has access to in the course of the computation. As an example, consider a double auction market with a Walrasian auctioneer who assembles supply and demand schedules from individual buyers and sellers to compute and announce *only* the cleared transactions and the market-clearing price. We underscore a strict confidentiality rule on individual supply and demand schedules to highlight the data privacy issues. Economically, this mechanism prevents trades from occurring away from the equilibrium price, thus avoiding a broad class of strategic behavior and helping to ensure a Pareto-efficient outcome.[22] If one assumes that the auctioneer is trustworthy then, almost tautologically, the auction will be carried out correctly, so that the auction mechanism leaks only the cleared trades and the equilibrium price, and nothing else.

More abstractly, fix a set of n parties $P_1, ..., P_n$ holding inputs $x_1, ..., x_n$, respectively. Imagine that these parties have agreed upon some collection of functions $f_1, ..., f_n$ that they would like to compute over their

[21] In practice, they are supplemented with more nuanced, human-applied rules such as need-to-know requirements, e.g. Obama [165, sec. 4.1]. However, if classification procedures grant access to an item, it is typically access to peruse the item in its entirety.

[22] Walras famously developed his model around the actual workings of the Paris Bourse; [23]. Verrecchia [198] discusses related issues of disclosure and reductions in informational asymmetries. For further discussion of the equilibrium properties of the auctioneer, see Rubinstein and Wolinsky [182] or Tesfatsion [196].

data, with party P_i being given the result $f_i(x_1, ..., x_n)$ and learning nothing else.[23] Furthermore, no one external to the protocol (e.g., an eavesdropper) should learn anything either. It is immediate that this can be done if the parties have access to a trusted party; each party P_i sends an input x_i to the trusted party (we assume this is done over an ideal channel, so that no one can look at or tamper with this value). The trusted party computes $y_1 = f_1(x_1, ..., x_n), ..., y_n = f_n(x_1, ..., x_n)$ and sends y_i to P_i.

Note that this solution not only provides security against individual cheaters, but also ensures security, even if several parties are colluding throughout the entire execution. If parties in some set S collude, then the parties in that set learn the union of what they each learn individually, but nothing more. Given this formulation—specifically, with the constraints given that we want party P_i to learn $f_i(x_1, ..., x_n)$ exactly—the solution using a trusted party is the best one could hope for, and we will therefore take this as our "ideal world." In the real world, in contrast, there may not exist any trusted parties that all the players agree upon.

Protocols for secure computation provide a way for $P_1, ..., P_n$ to achieve the security guarantees of the ideal world without the involvement of any external entities. Indeed, the definition of secure computation involves an explicit comparison between the real-world execution of the protocol (in which the parties exchange messages amongst themselves) and the ideal world just described. Roughly speaking, *a protocol is "secure" if the actions of any colluding parties in the real world can be emulated by those same parties in the ideal world.* (Alternately, we may think of the protocol as providing a "virtual" trusted party that is guaranteed to follow its specified program and reveal only what it is explicitly instructed to compute and output.) As a corollary, any attacks that are impossible to carry out in the ideal world are impossible to carry out in the real world either.

This model is powerful, but not a panacea. The model's usefulness depends on the extent to which the task at hand can be completely specified, since the trusted party must follow a well-defined algorithm. Furthermore, the ideal model does not always capture all security concerns; see Section 4.1.4 for a discussion of some attacks that are possible, even in the ideal world.

4.1.2 Examples of Secure Computation

Almost any cryptographic problem can be cast as one of secure computation (even if that may sometimes be overkill for the problem at hand). For example, one could cast the problem of private communication from P_1 to P_2 as the problem of computing the function $f_2(x_1) = x_1$. Here, party P_2 has no input and party P_1 gets no output. A trusted party computing this function would effectively take a message from P_1 and hand it to P_2. While this is not very useful as far as constructing efficient encryption schemes, it does provide a conceptually useful way to think about the guarantees that encryption provides.

The double auction setting described earlier is a more interesting example. There, the function to be computed is, for participant i (buyer or seller), the cleared transactions (including the transaction price and counterparty) that this bidder will participate in. Alternately, the auctioneer might simply announce a clearing price and let partipants who wish to transact at that price announce their intentions. The auction example is not hypothetical; a Danish sugar beet auction is run using secure computation to replace the auctioneer (see Section 4.1.5).

As another example, consider the case (discussed in Section 2.2) of brokers who provide a layer of anonymity to protect the identity of dealers in certain markets, such as foreign exchange. The "participants" here are the set of all potential dealers (in practice, this set is not large; dealers must have pre-existing contractual arrangements to be part of the market, even anonymously). The role of the "trusted party" here is played jointly by the brokers, who find appropriate pairs of participants to transact based on requested trades and desired prices, without informing other participants of the trade, and without revealing anything about unsuccessful orders (that cannot be inferred from a given institution's successful trades). Implementing this functionality through secure computation would provide anonymity to dealers without the need to trust brokers' discretion.

[23] We remark for completeness that the output computed by these functions can be probabilistic, in which case the results can also be correlated.

A final example comes from Abbe et al. [1], who propose using secure computation to calculate aggregate statistics that support supervisory monitoring of threats to systemic stability without exposing the full portfolio details of individual institutions. There, the parties are a supervisor and a set of institutions. The institutions input portfolio and transaction details, while the supervisor inputs specific summary functions to be computed. Using secure computation, the institutions can limit the exposure of confidential information, while allowing the supervisor to select the summaries to use in a given circumstance.

4.1.3 Key Assumptions and Main Feasibility Results for Secure Computation

We do not discuss in any detail how protocols for secure computation are designed. For a tutorial, see Lindell and Pinkas [138]. We focus here on understanding how to use such protocols and the conditions under which such protocols exist. The preceding discussion implicitly covers how to use such protocols to solve a particular problem: solve the problem under the assumption that a trusted party is available, and then replace the trusted party with a secure-computation protocol run among the parties themselves. In this section, we outline the basic (theoretical) feasibility results for secure computation. In the next section, we summarize the state-of-the-art with regard to practical implementations.

Modern security definitions all proceed by comparing the real-world execution of some protocol to an ideal-world execution, as previously described. Reiterating, a given protocol is *secure* if the actions of a group of colluding parties in the real world can be emulated by those same parties in the ideal world. To obtain a formal definition, then, we need a model of the real and ideal worlds, and we must define what it means to emulate a real-world execution in the ideal world. Such details are beyond the scope of this paper; the interested reader may refer to, e.g., Goldreich [93] for details.

We have already described the ideal world in detail in Section 4.1.1, and this is the model we will use for the ideal world unless stated otherwise. This model provides the strongest formulation of the ideal world, and so protocols proven secure with respect to this ideal world satisfy the strongest set of security properties. Nevertheless, there may be good reasons to consider weaker ideal-world models, e.g., for better efficiency or because the strongest notion of security is unattainable. One example is *security-with-abort*, where the trusted party computes the function(s) correctly and privately as before, but can then be prevented by a misbehaving player from sending output to some subset of the parties. An "abort" of this type corresponds, in the real world, to malicious participants who stop participating in a protocol after they have learned their outputs but before "honest" players learn theirs. Deviations of this type are relatively benign and can often be handled via mechanisms external to the protocol.

As for the real-world execution of the protocol, there are several issues to consider:

- *Corruption threshold:* Perhaps the most basic question is whether there is any assumed bound on the number of parties who might collude in an attempt to disrupt the protocol and/or learn more than they should. This involves some assumptions—outside the cryptographic model—regarding the lengths to which parties will go in their attempts to subvert the protocol.
- *Assumptions on behavior:* A second question, often decided before the previous one, is whether it is assumed that all parties run the protocol honestly (but may then try to learn more than they are allowed by looking at the record of the protocol communication), or whether no such assumption is made and protection is afforded against arbitrary behavior. The first is called the semi-honest or honest-but-curious model, while the second is called the malicious model. The assumption of semi-honest behavior may be a reasonable in many scenarios. For example, a protocol may be executed among parties who basically trust each other (e.g., government entities) but are prevented from leaking information for reasons of classification, policy, or law. In other cases, it may be infeasible to modify the protocol being run due to software audits or other mechanisms.
- *Computational resources of the parties:* An issue that we have ignored until this point is what assumptions, if any, are made about the computational resources of the parties. A full discussion is out of scope here, but we note a key dichotomy, namely that security of some protocols is *information-theoretic* and does not make any assumptions on the computational power of the parties, whereas

other protocols achieve *computational* security based on the assumptions that (1) certain mathematical problems are "hard" to solve, and (2) that the parties have (known) bounds on their computational power. In practice, computational security typically works well, and the only question is to determine reasonable bounds on parties' computational power.[24]

- *Network and other assumptions:* The usual network model is that every party can send messages to any other party, i.e., there are point-to-point links between each pair of parties. In addition, it is usually (implicitly) assumed that each pair of parties shares any necessary cryptographic keys needed to encrypt and authenticate their communication. This is the network model we assume unless stated otherwise. Sometimes other network models may apply. An example might be one with only partial connectivity between parties (say, smartphones that all talk to a cloud provider, but cannot communicate directly with each other). A stronger model might be to assume the existence of a broadcast channel, which allows everyone to hear the messages sent by some party, or a public-key infrastructure (PKI) in which each party knows everyone else's public key.

Let n denote the number of parties running a protocol. The main feasibility results, for computation of arbitrary collections of functions, are:

- When cheating parties are assumed to be semi-honest, it is possible to obtain information-theoretic security against arbitrary collusion of any $t < n/2$ of the parties [16, 37].
- When cheating parties may be malicious, information-theoretic security against arbitrary collusion of up to $t < n/3$ of the parties is possible [16, 37]. If a broadcast channel is available, this can be extended to $t < n/2$ [178].
- The bounds above are all tight, even if only computational security is required. Specifically, security against $n/3$ malicious, colluding parties is not possible without broadcast or some means of implementing broadcast, and security against $n/2$ parties is not possible even if broadcast is given.[25] However, see next.
- The above discussion refers to the strongest ideal-world model we have been considering. We can recover feasibility if we consider the weaker notion of *security-with-abort*. Here, computational security is possible against malicious collusion of any $t < n$ of the parties [206, 94].

  We remark that this covers the interesting special case of *two-party computation* in which two parties wish to compute some function over their inputs, while each protecting sensitive data from the other.

For most applications of secure computation, protocols for this last setting (computational security-with-abort) make the most sense, because they require no assumptions on the number of honest participants. Indeed, state-of-the-art protocols generally provide this type of security (see Section 4.1.5).

4.1.4 What Secure Computation Does Not Provide

It helps to clarify what secure computation does not provide. By construction, secure computation cannot provide security guarantees that are not present in the ideal-world computation involving a trusted party. In particular, then:

- Secure computation does not prevent attacks based on a party lying about its input. For example, if the parties are implementing a first-price auction, then nothing forces a party to report its true valuation of the object as its input, and all the same game-theoretic considerations that are present in the ideal world remain when a secure protocol is used. As another example, if several firms are pooling information about their customers' purchasing habits, nothing prevents one party from using fake customer information if that will provide an advantage (for example, by giving erroneous results

[24] Indeed, even protocols with information-theoretic security require (in practice) messages sent as part of the protocol to be encrypted using an encryption scheme that is only computationally secure.

[25] It is known that a PKI suffices to realize a broadcast channel, with computational security.

to the other parties). There may be ways to enforce the use of correct inputs (or verify inputs), but they would require an external source of information allowing the protocol to verify the inputs.

- Secure computation reveals to each party its prescribed output *along with anything that can be deduced from that output* (in conjunction with that party's input). A simple example might be a first-price auction in which only the winner, but not the winning bid, is announced. In that case everyone learns the winner, and the winner additionally learns an upper-bound on everyone else's bid. An important first step to using secure computation is thus to decide what leakage is acceptable in the first place (i.e., even in an ideal world involving a trusted party). See Section 4.2 for further discussions along this line.
- The above concerns may be magnified in the event of collusion. If several parties collude they may jointly set their inputs any way they like in an effort to maximize their advantage, and can attempt to deduce information from the union of their outputs. It is easy to find examples in which each party's output individually reveals nothing sensitive, but the collection of two or more parties' outputs does.
- Secure computation requires that the trusted party's desired behavior be precisely specified as a computer program. However, there are many situations where the processing to be done on the secret data requires considerable human judgment (for example, on the part of an auditor); such situations require a more subtle use of secure computation (having the trusted party perform only part of the task, for example).

4.1.5 Specific Instantiations and Current State-of-the-Art

Over the past decade, secure computation has moved from the realm of computer science theory to actual implementation. For example, Danish farmers deployed secure computation in 2008 to find the market clearing price for contracts on sugar-beet production via a double auction [31, 32, 33]. Reminiscent of the Walrasian auctioneer described above, each buyer (typically a sugar producer) or seller (typically a sugar beet farmer) specifies the quantity he is willing to buy (resp., sell) as a function of the price. Based on these individual supply and demand schedules, the "auctioneer"—implemented by a secure-computation protocol to protect individual bidder information—computes the market-clearing price. This particular implementation utilizes a three-party protocol with parties representing: (1) the only sugar-beet processing company in Demark, with whom the contracts were executed; (2) an association representing the sugar-beet farmers; and (3) the research organization who developed the secure protocol.

In another, more recent implementation, Bogdanov et al. [30] describe a working system that aggregates unaudited semiannual financial statistics for Estonian firms to support reporting by the Ministry of Economic Affairs and Communications.

The state of the art in implementation is advancing quickly, with a flurry of recent activity (e.g., [184, 143, 137, 15, 116, 140, 129, 115, 160, 175, 106, 139, 141, 189, 110, 132, 44, 161, 111, 14, 80, 81, 96, 154]). As of this writing, a rule of thumb is that current implementations of secure computations between two parties over a fast network in the "semi-honest" model are roughly a factor of 10^4 slower than the time taken to compute the trusted party's function directly (without secure computation) on similar hardware [188]; a computation that takes normally takes milliseconds on a desktop would take tens of seconds via secure computation. This means that secure computation is already practical for simple, infrequent calculations (such as those involved in most regulatory data sharing). This slowdown is likely to decrease as protocol design improves.

4.2 Statistical Data Privacy

Many cryptographic tools provide the functionality of a trusted party (see Section 4.1) that transmits, stores, and processes information on behalf of participants in a protocol. These are powerful tools for situations in which bright lines separate the sets of participants to whom different pieces of information should be available. In many such settings, however, it is not clear what should be revealed to whom; one must first understand when revealed information might allow an attacker to *infer* sensitive information. Techniques

of statistical data privacy emphasize the latter problem. Such questions of privacy and confidentiality are often orthogonal to the implementation of a trusted party. In the language of the previous sections the key question becomes "*What should the trusted party compute?*" and "*What facts should remain concealed?*," or, "What might be unintentionally revealed by seemingly innocuous published information?"

One highly prominent and relevant setting for economic research and regulations is individual privacy in statistical releases. Collections of personal and sensitive data, previously the purview only of statistical agencies, have become ubiquitous. Increasing volumes of personal and sensitive data are collected and archived by health networks, government agencies, search engines, social networking websites, and other organizations. Much research has explored releases such as this in several scientific fields: databases, data mining, machine learning, and cryptography among others. The broad question is, how can we glean the benefits of research based on these datasets without compromising the privacy of individuals whose information they contain? The challenges are complex and typically context-dependent, and there is no consensus yet on an unambiguous "right way" to approach these problems.

Several high-profile failures of supposed anonymization schemes demonstrate that simply removing obvious identifying information, such as names and addresses, is *not* sufficient. For example, in 2006, AOL, an Internet service provider, released a corpus of web search queries to aid research on search engine optimization. User names were removed from the dataset and replaced by random identifiers. Nevertheless, the ability to link the searches of any given user made it easy to reidentify users from the search logs [12]. Even seemingly aggregate statistics may pose subtle challenges. Consider a university that reveals the average salaries of each of its departments every month. If in some month the only change in a department's staff is the hiring of Professor X (and if the total number of staff in the department is known), then comparing the average salaries before and after X's hiring would reveal the new professor's starting salary. The *security of the method used to collect salaries and compute their average is irrelevant*; the problem is inherent in the release.

Financial data collections raise confidentiality issues, such as the protection of institutional trade secrets, that go beyond concerns with individual privacy and PII. We focus here on individual privacy in statistical databases because this approach offers lessons for the management and use of financial data, and because it is currently the only setting in which substantial theoretical and practical results are available.

4.2.1 Current Practice

Many government agencies collect personal information and release data products based on that information. There are two basic models for making data available for analysis: the "data center" model, which makes a restricted facility available (on-site or online) to selected researchers whose results are manually inspected before they are allowed out of the facility; and the public release model, in which "data products" (typically either summary statistics or fine-grained microdata) are published for unrestricted use by the public. We focus on the public release model in this paper.

Existing methodology for protecting individual privacy in those releases varies tremendously across agencies, and a survey of current practice would be well beyond the scope of this work. Techniques for making releases private include, (1) "perturbation," in which data points are changed, perhaps by the addition of some noise or the swapping of entries in a table, (2) "generalization," in which individual values are replaced with a label representing a set of values; for example, exact ages could be replaced with a five-year range such as 30–35, and (3) the release of summary statistics that involve computation across multiple records. Releases are often made available to the public online (e.g., the Census Bureau's American Factfinder [104]). A high-level description of practices at U.S. federal agencies can be found in "Statistical Working Paper 22" [69]; see Zayatz [208] for further discussion specific to the Census Bureau.

The procedures for deciding whether a given release is sufficiently private are complex, and rely on case-by-case analysis and judgment by experts. Zarate and Zayatz [207] provide examples of successful disclosure review procedures (see also [69]). The main operating principle is to prevent *reidentification*, that is, the matching of particular records in a release to real-world individuals. The process of modifying the data is thus often called "anonymization." Because reindentification is often done by matching records based on specific information (age, address, etc.), current regulations rely heavily on protecting "personally

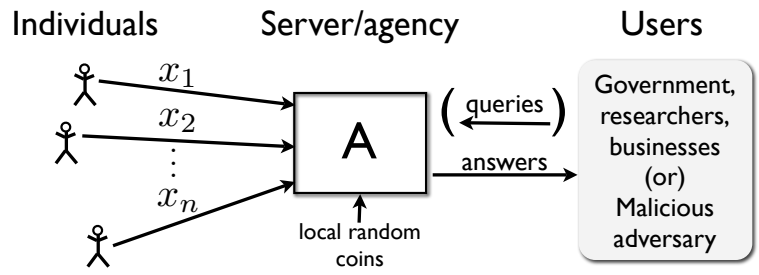

Figure 2: The trusted agency model. In *one-shot* protocols (mechanisms), the users send no queries, and there is simply one message from the server to users.

identifiable information" (PII).

As we discuss in Sections 4.2.3 and 4.2.4, the explosion of data available about individuals has made anonymization and PII extremely problematic. Although the disclosure control methodologies embodied in current practice and regulation have thus far successfully prevented privacy breaches based on government data publication, these methodologies rely on inherently fragile concepts, such as anonymity and PII, and—except in a few cases [207]—require individual human review of potential releases. In particular, the difficulty in defining PII makes it hard, if not impossible, to enforce.

4.2.2 A Trusted Agency Abstraction

To make the discussion more precise, we focus on a simple, stylized model of interaction, illustrated in Figure 2. Individuals give their data to a trusted, central agency (such as the Census Bureau, or a financial data vendor), which processes the data $x = (x_1, ..., x_n)$ and makes the results available to (possibly malicious) end users. The role of the trusted agency here is essentially the same as that of the trusted party described above in Section 4.1: the trusted party/agency reliably coordinates communication among participants in the system without permitting information leakages or disclosures other than those agreed by the parties in advance. Such agreed disclosures may be quite complex, for example, allowing arbitrary questions within a given, constrained class of queries.[26] In an interactive protocol, users ask questions and get replies. In a noninteractive protocol, the agency processes the data and publishes a single digest $A(x)$ once and for all.

This simplified model also highlights why the problem addressed in this section is fundamentally different from SFE discussed in Section 4; [94]. The techniques of SFE eliminate the need for a trusted party by distributing computations among a set of computers without revealing anything except the desired outcome. However, this model does not study whether the desired outcome is itself safe to reveal. Statistical data privacy and secure multiparty computation (i.e., SFE) are thus complementary technologies that should benefit from being used in concert. We return to these issues in the international data sharing example in Section 5.3.

A variant of this model is the *randomized response*, also called the *local* model, because it does not rely on a central trusted party (ideal or real) for secrecy. In this model, an individual's private information x_i is never directly processed; instead, a suitably randomized version $R(x_i)$ is stored (and can even be transmitted directly to users). Thus, the outcome of the mechanism is $A(x) = (R(x_1), ..., R(x_n))$, in which R is a randomized algorithm agreed as part of the protocol. This model originated in 1960s to help surveyors gather accurate answers to sensitive questions [200], but it is a popular model for privacy as well, particularly in the context of online surveys (see [3] and many follow-up works, notably [64]). Although these examples involve randomization of data at the point of survey reponse (e.g., to a CIPSEA agency, as described in

[26] Obviously, if completely arbitrary queries are allowed, then no privacy is possible. Similarly, allowing arbitrarily long sequences of questions from certain restricted query classes may be too revealing; this is the essence of the familiar parlor game of "20 Questions."

Section 3.1), agencies also frequently use randomization techniques at the point of disclosure of information to the general public. Randomization is part of a broader class of tools—including various flavors of rounding, bucketing, and top-/bottom-coding—that separately alter individual data points to disclosure, while trying to minimize any bias that the alteration might introduce.

4.2.3 Linkage and Reconstruction Attacks, and the "Myth" of PII

Over the last decade, a number of publicized breaches of privacy due to the release of supposedly anonymized information highlighted the difficulty of "anonymizing" data. Almost all of the attacks were based on some kind of external knowledge (also called *backround knowledge, side information*, or *auxiliary information* available to an attacker).

Many such attacks work by linking records in a supposedly anonymized dataset with identified records available elsewhere. One study [195] identified the governor of Massachusetts in a medical database anonymized in this simple-minded manner. A New York Times article [12] exposed a searcher in supposedly anonymized search data released by the Internet service provider AOL. Users of the film rental service Netflix were identified from similarly anonymized movie ratings data [155]. The provided data were combined with information available in other public databases to answer a million dollar challenge by Netflix in a fraudulent manner. In all three cases, there was no break into the database by hackers; the organization holding the database violated privacy by incorrectly assuming that it was publishing only safe information.[27]

More recently, similar techniques have been used to deduce information about individuals from supposedly anonymized releases in a wide range of contexts: (1) to link individuals to nodes in deidentified social networks [9, 156], (2) to reidentify accounts on a photo sharing website [158], (3) to reconstruct the topology of a computer network from anonymized network traffic data [41, 179], (4) to link mobile location traces to social network accounts [190], and (5) to identify participants in clinical genetic studies [108, 101].

These attacks demonstrate the extreme difficulty of distinguishing between "identifying" and "nonindentifying" information. A large number of seemingly innocuous pieces of information, taken together, may provide a unique fingerprint that can be used to link a particular record to some other data source. It is important to note that the privacy laws discussed above (Section 3) typically constrain the handling only of the information that a given organization itself controls, regardless of the type(s) or amount of background knowledge that might be available elsewhere.

In this sense, almost everything is personally identifiable information. For example, none of the information in the AOL Web search queries of Ms. Arnold (the victim of the privacy breaches described in [12]) would be classified as PII according to the Health Information Portability and Accountability Act; yet it was quite easy to identify her from them. Black-and-white classifications of any information as "anonymous" or "identifying" should thus be treated with circumspection, if not downright skepticism. For a longer discussion of this issue, see the essay of Narayanan and Shmatikov [157].

The attacks described above hinge on releases that reveal the exact information of some subset of records. It is tempting to conclude that the problem stems from the release of highly granular, individual-level information (such as a list of a user's film ratings). However, even coarse-grained, seemingly high-level information can reveal individual attributes. For example,

- *"Global" results that single out individuals* - In some cases, the results of global processing of a dataset can themselves encode individual information. An obvious example is a release that describes the outliers in a dataset. A more subtle example is a support vector machine (SVM), a particular method for designing linear binary classifiers. The output of a SVM is typically described by a set of data

[27] In a less sophisticated case dealing specifically with banks, Flood [79, p. 31] attempted to reverse-engineer the specific identities of 15 large banks reported by the FDIC to have high supervisory CAMEL ratings. (The CAMEL rating is an acronym—later expanded to "CAMELS"—for a composite index of bank quality on an integer scale of 1 to 5; lower numbers are better. A bank's rating is assigned by examiners and is RSI.) He succeeded with a high degree of accuracy by linking the published aggregates with (public) balance sheet and income statement data and with basic institutional facts about the calculation of risk-based deposit insurance premia.

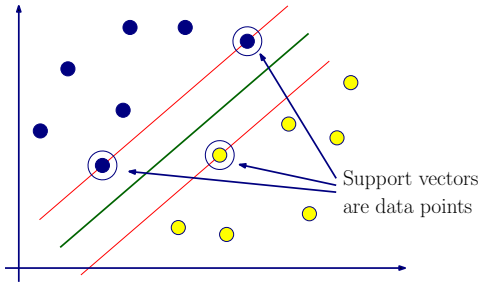

Figure 3: The half-plane classifier returned by a support vector machine. Circled data points are the "support vectors" used to describe the dual form of the solution.

points, listed "in the clear," that define the hyperplane corresponding to the classifier (see Figure 3). Thus, an apparently very global computation reveals exact data about a particular set of individuals.

- *Multiple related releases* - As mentioned earlier, the average salary of a department before and after a particular professor is hired reveals the salary of the new hire. This type of issue arises especially easily with longitudinal data (i.e., data for a fixed set of respondents measured and released over time), but also comes up with independently constructed releases about related groups (e.g., hospitals that serve overlapping populations).

- *Reconstruction attacks* - Another class of attacks uses multiple seemingly unrelated global releases to reconstruct sensitive data. The idea is that every release about a dataset, even a noisy one, introduces a constraint on the set of possible actual datasets. When combined, a large number of constraints may (nearly) uniquely determine the dataset. This phenomenon has been analyzed extensively [48, 55, 61, 58, 120, 46] for releases that induce linear constraints. Moreover, many natural statistical releases (such as regression coefficients) can be used to derive linear constraints [121].

  For a simple example of a reconstruction attack, consider a dataset x in which each person's data consists of a single bit x_i (say, whether or not person i defaulted on a mortgage). The dataset is thus a vector $x_1, ..., x_n \in 0, 1^n$. Suppose we want to release a summary of the data that allows one to reconstruct, for any subset S in$\{1, ..., n\}$, the approximate number of 1s in positions in S (that is, $\#\{i \in S : x_i = 1\} = \sum_{i \in S} x_i$).

  For each subset S, the corresponding count $C(S, x)$ can be thought of as a linear constraint on x (it is the inner product of x with a vector which has 1s in the positions corresponding to x and 0s elsewhere). If the exact values of many of these counts are released, then one can reconstruct x simply by solving the corresponding linear system of equations. Reconstructing the entire secret vector x is possible (roughly) once n counts have been released.[28] Even if the counts are not released exactly, but with some error introduced intentionally, one can exploit the significant literature on solving noisy systems of linear equations to recover a very good approximation to x.

  Reconstruction attacks highlight that there is no free lunch when releasing statistics about sensitive data: answering too many queries too accurately allows one to reconstruct the data. *Publishers of aggregate data must thus choose to release some summaries at the expense of others.* In particular, it is often not possible to generate data products containing "all" of the relevant information.

[28] More precisely, one needs n counts for which the corresponding vectors are linearly independent. Linear independence is typical, though. Random queries, for example, satisfy linear independence with overwhelmingly high probability.

4.2.4 Initial Attempts to Pin Down "Privacy": k-Anonymity and Query Auditing

Attacks such as those outlined earlier motivated the development of sanitization techniques to prevent the attacks. Some attempts, such as the well-known notion of k-anonymity [195], restricted the form of the output with the goal of preventing specific types of linkage attacks. Later notions, exemplified here by differential privacy, restrict the process that generates the output, and provide rigorous guarantees that any algorithm satisfying the definition would provably protect a well defined notion of "privacy" under well specified assumptions. (We restrict our discussion here to specific examples from the academic literature; many of these have parallels in official statistical practice.)

It is instructive to consider first the initial efforts to pin down a class of reasonable sanitization algorithms. An example is k-anonymity [195], which requires that values in a published table be generalized so that every row appears at least k times in the dataset (think of k here as a small value, say 5). Generalization involves replacing specific values with more general categories. For example, we might replace an exact age (say, 35) with a 10-year range (30-39). (In an interesting coincidence, this type of discretization was also used to reduce information asymmetries in the diamond market—see Section 2.2.) k-Anonymity is designed to prevent a particular type of linkage attack; the idea is that any record from another database will match either no records at all or at least k records.

As a general approach to privacy, however, k-anonymity and its variants pose several challenges.

- *Revealing low-entropy values* - If all records in a group have the same value of some particular field (say, gender) then that value is revealed exactly.
- *Sensitivity to side information* - Suppose that mortgage loan information is released and aggregated into geographic units consisting at least k loans. If an attacker already knows about the $k-1$ other loans in the group (say, the loans on a particular block), the attacker can deduce quite a bit about the remaining loan.
- *Composition* - Even for large k, independently anonymized releases of datasets concerning the same individual may be combined to learn exact information [84]. For example, suppose two hospitals independently release information about overlapping populations and that Alice visited both hospitals for the same condition. Alice's employer could easily learn a list of k possible conditions from each of the releases. The intersection of the two lists will typically contain far fewer than k conditions.
- *Choice of generalization algorithm* - More subtly, the definition places no restrictions on the algorithm used to group data points. The grouping algorithm could unintentionally reveal a lot by the choice of elements that were clustered together. For example, see [204].

A wide range of approaches proposed in the database literature (many based on "auditing" queries to look for bad interactions between queries) suffer from similar challenges. To give a flavor of what may go wrong, note that auditing systems may reveal information about the data, not only through the answers to the queries they allow, but also through the decisions to deny queries, if those decisions are based on an inspection of the data. For a survey of the literature, see Adam and Wortmann [2] and, for a discussion of some of the difficulties, see Kenthapadi et al. [126].

These foregoing issues surrounding the problematic notions of PII and anonymity have motivated the search for more mathematically rigorous and potentially automatable methods. In the remainder of this section, we discuss ideas from the academic literature that offer a very different approach.

4.2.5 Rigorous Foundations: The Case of Differential Privacy

The preceding discussion reveals several salient lessons:

- Side information is difficult to reason about, and it is impossible to know exactly what side information might be available in the future.
- One must reason about the process (or algorithm) that generates outputs, not only the form of the outputs themselves.

- "Sanitization" is not a black-and-white concept. The reconstruction attacks show that any sufficiently rich collection of sanitized statistics, even highly aggregate, can be used to reconstruct sensitive data.

The challenges faced by approaches like k-anonymity and auditing motivated researchers to seek more principled approaches to the problem. One successful approach, which we discuss in detail here, is *differential privacy* [60, 50], which arose from a line of work in cryptography and theoretical computer science [48, 55, 25]. Differential privacy places conditions on the *algorithm* A run by the agency to generate output (either as a one-shot publication or an answers to queries). This approach is not a specific algorithm or technique — indeed, there can be many differentially private algorithms for a particular type of release.

The basic idea of differential privacy is to require that the output of an algorithm A that processes a dataset $x = (x_1, ..., x_n)$ be nearly "the same" regardless of whether any particular entry x_i is included. More precisely, we think of the process A that releases the data as *randomized*. The randomization might come, for example, from noise addition or subsampling. Differential privacy requires that for any given dataset x and individual i, the *distributions* on the outputs of $A(x)$ and $A(x')$ be close, where x' is a version of x from which person i's data has been removed.

Intuitively, this requirement implies that any conclusions an adversary draws from seeing the output $A(x)$ do not depend heavily on any one individual's data. An important subtlety here is that while much might be learned about an individual, whatever is learned would be the same *whether or not that person's data were used*. Moreover, this result holds no matter what an attacker knows ahead of time. In this sense, this result provides a meaningful guarantee in the presence of arbitrary side information.

Privacy guarantees can be subtle to interpret. For example, if Alice's employer, Bob, knows ahead of time that she smokes, then a study on the relationship between smoking and cancer might lead Bob to conclude that Alice is at a higher risk of lung cancer than he previously thought. In that sense, Bob learns significant information about her. But Bob learns this whether or not Alice participated in the study. Differential privacy disentangles the inferences Bob draws from learning about the population as a whole from the inferences he draws that are specific to a particular individual.

Formalizing differential privacy is delicate; we provide some basic definitions here to make the discussion more concrete.[29] Suppose each individual contributes a value $x_i \in D$ to the database, where D is some possibly complicated set (e.g., x_i could be the individual's tax returns, voice print, census answers, e-mail usage, etc). For every database $x \subseteq D$, the (randomized) privacy mechanism A defines a random variable $A(x)$ on the output space. We say two datasets $x, y \subseteq D$ are *neighbors* if they differ only in a single individual's data, that is, $|x \triangle y| = 1$ where $x \triangle y$ denotes the symmetric difference of the sets x and y. The mechanism A is private if neighboring datasets induce nearby distributions on outputs:

Definition 1 (ϵ-differential privacy [60, 50])**.** *A randomized algorithm A is ϵ-differentially private if for all neighboring pairs $x, y \subseteq D$, and for all sets S of possible outputs,*

$$\Pr(A(x) \in S) \leq e^{\epsilon} \times \Pr(A(y) \in S)\,.$$

The parameter ϵ can be thought of as a measure of information leakage. It is a measure of how far apart the distributions of $A(x)$ and $A(y)$ can be when x and y differ in only one person's data. (The exact choice of distance measure is important for the definition to be meaningful—see [60] for a discussion). In typical applications, ϵ is less than 1 (say 0.1 or 0.01). A variant of the definition, called (ϵ, δ)-differential privacy [59], includes an additive error term δ (in addition to the multiplicative error ϵ); the difference between these definitions is not important here.

Differential privacy satisfies a number of useful properties, such as *composition*: if t different ϵ-differentially private algorithms $A_1, A_2, ..., A_t$ are run on overlapping datasets, then their joint output is (at most) $t\epsilon$-differentially private [59]. Thus, if many different organizations release information about the same individual, then privacy guarantees will degrade gracefully (unlike k-anonymity, discussed previously, in which one can lose anonymity completely with just two releases). Note that some degradation is necessary if the

[29] The reader not interested in understanding the technical details may skip the remainder of this section without losing the general thread.

algorithms provide useful statistical summaries. The reconstruction attacks described earlier demonstrate that one cannot answer too many queries too accurately without revealing the dataset entirely.

The types of guarantees provided by differential privacy in the presence of side information are discussed at length in the literature. Kasiviswanathan and Smith [119] provide a Bayesian formulation of the guarantee. Dwork and Naor [54], Kifer and Machanavajjhala [127] show that any useful algorithm must allow inferences about individuals in the presence of side information (as the smoking and cancer example earlier illustrates); the "relative" guarantee provided by differential privacy is, in many settings, a reasonable compromise.

4.2.6 Some Applications

Differentially private algorithms cannot provide perfect accuracy for most summaries. The definition requires that the algorithms introduce enough uncertainty to cover the change caused by the insertion or removal of an individual. Moreover, as the reconstruction attacks show, it is not possible to design a single, one-shot release algorithm that can answer any possible set of queries. Nonetheless, differentially private algorithms have been designed for a wide range of statistical and machine learning tasks, as have algorithms that produce "synthetic" data supporting a large set of specified queries.

The literature on differentially private algorithms is too vast to survey here. A number of surveys in the last few years give an account of ongoing developments in the design of differentially private algorithms [51, 52, 57, 180]. Even these surveys are only partial; the state of the art is evolving quickly. The overarching theme is that aggregate statistics that are "insensitive" to changes in individuals' data can be released fairly accurately, while satisfying differential privacy. In contrast, statistics that depend heavily on individuals (for example, a listing of data points that are outliers according to some measure) cannot be revealed while satisfying differential privacy. A consequence is that one must often design new, more robust algorithms for common analytical tasks. Techniques for designing these algorithms include noise addition and random subsampling, as well as much more sophisticated sampling algorithms. For an introduction, see the survey of Dwork and Roth [56].

A recent line of work has investigated the connections between economic theory and differential privacy. Although none of these works directly addresses issues with regulatory data, they provide strong connections between privacy and game-theoretic microeconomic questions. For example, several works use differential privacy to design incentive-compatible mechanisms for auction and allocation problems, starting with McSherry and Talwar [149] (see also [205, 38, 163, 164, 112]). A different line of work uses differential privacy for equilibrium selection [123]. These works have in common a "game-theoretic" interpretation of differential privacy, namely, if individuals can choose the values to report as their input to a differentially-private mechanism, they have very little to gain (the amount depends on the parameter ϵ) by lying. It is thus an (approximate) equilibrium for all players to report their true values. This idea is also at the heart of a line of work on *pricing* privacy by asking participants to pay (or be rewarded) differently depending on ϵ (see, e.g., [92, 135, 181, 78] as well as the survey of Pai and Roth [171]).

In addition to a large number of works on methodology and algorithm design, a number of papers have investigated specific applications, such as plotting spatial data [142, 39] (the latter provides an interactive demonstration), frequent item set mining [20], network trace analysis [147], and recommendation systems [148].

As the "smoking and cancer" example highlights, differential privacy does not prevent inferences that come from learning global information (i.e., information not specific to an individual, such as the relationship between smoking and lung cancer). This problem is in some sense unavoidable. Any information that allows the analyst to learn something about the world will, in some circumstances, change the inferences made about individuals [54, 127]. However, this issue has important implications for financial data; for example, aggregate statistics about individual transactions might reveal sensitive information about a firm's trading strategy or position. We discuss this problem further below.

A number of variations on, and generalizations of, differential privacy have appeared in the literature [128, 21, 88, 89, 102]. The most relevant here is the Pufferfish framework of Kifer and Machanavajjhala [128], which generalizes differential privacy by allowing one to specify the type of information to be kept secret, and the assumptions one is willing to make about available auxiliary information. Given these assumptions,

one gets a specific notion of privacy (which a given release algorithm may or may not satisfy). There is no automatic way to generate algorithms that satisfy the definition and provide useful results; a case-by-case analysis is still required. Also, as mentioned above, quantifying the available auxiliary information is delicate, at best.

4.3 Confidentiality Guarantees for Financial Data

How should the notions of the preceding section apply to financial data? There are, crudely, two main concerns with regulatory data: individual privacy and institutional confidentiality. As mentioned earlier, the literature on statistical data privacy focuses on individual privacy. The notions developed in that context (such as differential privacy) are useful when the principal concern is privacy of individual investors (such as for the release of datasets on home loans, as in Section 5.2). Institutional confidentiality is more complicated. A release that hides individual investors' information might still reveal confidential information about a firm (trading desk portfolios, for example); firm-level trade secrets might not be sensitive to changes in individuals' data.

A simple way to approach the issue is to think about what types of *changes* to the datasets should not be visible to an outsider viewing the released information. (In the language of differential privacy, which datasets do we take to be neighbors?) The set of allowed changes corresponds roughly to the type of information hidden [128]. We suggest here two variations on differential privacy that could be appropriate for addressing firm-level confidentiality concerns:

1. *Firm-level privacy* – This would require that the removal or modification of any single firm's data not affect the release significantly. It might be possible to provide this type of privacy for extremely coarse statistics, such as financial stress indexes (Section 5.1). However, in general, there are large firms whose removal would significantly alter market statistics, that is, they have no crowd big enough to hide in.

2. *Limited-precision, firm-level privacy* – When some firms are too big to hide, the following more restricted notion might make sense: two datasets are considered neighbors if they differ in the reallocation of up to T dollars of one firm's portfolio. As before, we would require that neighboring datasets be hard to distinguish.

   Any firm whose total portfolio value falls below T would be completely hidden in such a release (that is, such a firm would not affect the output distribution), whereas larger firms would protected, roughly, up to precision T (positions with value below T would be hidden, those above T would be visible). The question of an *a priori* appropriate value for T would be a policy decision, but a rough rule could be the size of the 100th largest bank, or something similar. The value of T would depend on the specific release; a key issue would be to calibrate T to provide an "optimal" transparency-confidentiality tradeoff. An open question is whether such a threshold would in fact provide the benefits of confidentiality (e.g., protecting trade secrets).

5 Three Use Cases

In this section, we offer three specific usage scenarios as illustrations of how the new privacy techniques might be applied to specific challenges for financial regulation and disclosure.

5.1 Publication of Aggregated Sensitive Data

5.1.1 Background

Since the recent crisis, a number of financial regulators have initiated the publication of indexes of financial conditions. Prominent examples include the four new financial stress indexes now published by various Federal Reserve Banks [169, 38–45], an index for Canada [113], and indexes that the IMF has constructed

for various countries. All these measures aim to condense the state of an enormously complex financial system into a single number that can be tracked through time. We will refer to any such aggregate as a *financial conditions index* (FCI).

Regulators compute FCIs based on several types of information:

- public data, without any restriction on use or disclosure (e.g., gross domestic product),
- licensed data, governed by intellectual property rights and contractual provisions of an agreement with a data vendor (e.g., prices and quotes acquired from a data vendor),
- individual private data, restricted by government privacy laws (e.g., PII on a personal loan application or contract), and
- confidential data, restricted by government laws or rules on confidential business information (e.g., RSI such as details of trading desk portfolios).

Current FCIs are based on only public data; legal restrictions forbid direct disclosure of each of these other types of information.[30]

However, indexes that incorporate confidential data can be much more accurate. For example, Oet et al. [167, 168] compared an index based on both public and confidential data (Systemic Assessment of Financial Environment, SAFE) with an analogous index based only on publicly available data (Cleveland Financial Stess Index, CFSI). Their analysis indicates that the confidentially augmented SAFE index would have been a significantly more accurate indicator at the height of the recent financial crisis (see Oet et al. [166, Figure 4]).

5.1.2 Usage Scenario

The Federal Reserve Bank of Cleveland's SAFE and CSFI illustrate two extremes: compute an "unencumbered" FCI based on fully public data that can be released, but has relatively low statistical accuracy, or compute a "confidential" FCI that incorporates confidential data and is more accurate, but cannot be released.

We propose computing a "sanitized" index that is based on both public data and confidential information—and hence, more accurate than the unencumbered FCI—yet comes with rigorous privacy guarantees for the confidential data. The most relevant concerns here are institutional confidentiality, and we conjecture that reasonably accurate indexes are possible satisfying *firm-level* differential privacy (Section 4.3). The magnitude of the effect of specific large institutions on the data is hard to judge without a careful review of the exact computations used (minor changes, such as the normalization of certain quantities by firm size or the removal of outliers have a pronounced effect on the "sensitivity" of the index to specific firms). Further understanding of this issue remains an important open question: "To what extent would *limited-precision* firm-level privacy suffice to capture concerns about institutional confidentiality?"

5.2 Retail Loan Information to Support Research

5.2.1 Background

Regulators collect highly granular datasets on retail loan exposures, including home mortgages and credit cards.[31] The datasets are large by econometric standards, containing tens of millions of records, and high-dimensional, carrying detailed information about accounts and borrowers. Supervisory analysis would benefit

[30] It is typically possible to negotiate permissions for public release of snippets or derived depictions and aggregations of licensed data, but much less flexibility is available for PII and RSI.

[31] For example, the Federal Housing Finance Agency and Consumer Financial Protection Bureau plan to assemble and refine collaboratively a National Mortgage Database to support both policymaking and research [40]. To support bank stress testing under its Comprehensive Capital Analysis and Review process, the Federal Reserve assembles loan-level detail on first-lien home mortgages and home-equity lines of credit [27]. The Office of the Comptroller of the Currency maintains a Consumer Credit Database of retail borrower information [177].

greatly if the data could be shared with the broader research community. However, sharing the raw data is problematic. The information in the datasets is extremely sensitive, and vast amounts of "side information" about the datasets are available through public records, raising the possibility of reidentification and sensitive inferences, even if the data are anonymized. At the same time, most issues of supervisory concern do not involve individual borrowers per se. The datasets' value lies in aggregate patterns, such as geographic and demographic trends in product usage, or expected default and delinquency behavior.

5.2.2 Usage Scenario

The main confidentiality issue with data of this type is individual borrowers' privacy, and so the tools developed for statistical data privacy can be used here. Because so much side information about housing loans is available through public records, it is definitely *not* sufficient to remove obvious identifiers from the data. In this application, methods with strong privacy guarantees (differential privacy or related notions) seem the best fit, at least for any datasets that will be accessible to a wide range of researchers.[32]

Applying such methods generally requires understanding the classes of computations researchers will want to apply. As mentioned in the discussion of reconstruction attacks, it is provably impossible to preserve *all* statistical features of a dataset, while providing privacy. A good set of candidate statistical features to preserve is the set of correlations (interactions) among small sets of attributes (see Barak et al. [11], Hardt et al. [103] for examples of such releases), as well as linear relationships (necessary for linear and logistic regression models). Releases of retail loan data present a challenging test for the state of the art in statistical data privacy.

Finally, it is worth investigating whether there are any additional *institution-level* privacy concerns that may arise.

5.3 International sharing

5.3.1 Background

In April 2009, during the depths of the recent financial crisis, the Group of Twenty (G-20) launched a "Data Gaps Initiative" to identify and close supervisory information gaps system-wide.[33] In the words of its 2009 report [74, p. 4], "the recent crisis has reaffirmed an old lesson—good data and good analysis are the lifeblood of effective surveillance and policy responses at both the national and international levels." The initial report contains 20 recommendations, including two specifically on sharing data about individual institutions with international groups of supervisors, called *colleges* ([77, Recommendations 8 and 9, p. 7–8]).[34] The FSB has already begun centralizing and sharing data, relying on highly restrictive access controls and physical security protocols to maintain confidentiality.

The recommendations also highlight the confidentiality concerns raised by sharing data internationally. Concerns that exist domestically are exacerbated with international sharing, because of limited cross-border authority to enforce agreements and govern disputes and misunderstandings. For example, privacy laws vary from one country to the next; a disclosure that is innocuous in one jurisdiction might be illegal in another.

[32] Access to the raw data for a smaller set of researchers might be enabled through on-site research facilities of the type used by the Census Bureau or the Internal Revenue Service.

[33] Specifically, the G-20 Finance Ministers and Central Bank Governors Working Group on Reinforcing International Co-operation and Promoting Integrity in Financial Markets called on the International Monetary Fund (IMF) and the FSB to explore information gaps and propose responses [74]. The IMF and FSB staff have produced approximately annual progress reports: [75], [76], [77].

[34] Basel Committee on Banking Supervision [13, p. 1] defines supervisory colleges as "multilateral working groups of relevant supervisors that are formed for the collective purpose of enhancing effective consolidated supervision of an international banking group on an ongoing basis." Principle 3 states, "College members should make their best efforts to share appropriate information with respect to the principal risks and risk-management practices of the banking group. Mutual trust and relationships are key for effective information sharing. Nonetheless, formal confidentiality agreements, such as contained in Memoranda of Understanding (MoUs), among college members facilitate this process." See also Alford [5].

Similarly, rules can change. Sharing might occur willing initially, but become a source of regret after changes in access or disclosure rules.

5.3.2 Usage Scenario

This use case raises two separate issues: First, "How can these summaries be computed to avoid losing sovereign control over confidential information?" Second, "What is revealed about specific financial institutions by the (minimal) summaries that colleges of regulators need to make informed decisions?"

The first issue can be addressed using multiparty computation (Section 4.1). As suggested by Abbe et al. [1], different agencies can jointly simulate a trusted party that will perform a particular computation (for example, Herfindahl-Hirschman Indexes, HHIs) without actually pooling their data in one place. (The particular protocol suggested by Abbe et al. [1] is no longer the state of the art, either in terms of efficiency or security. For a discussion of the (quickly evolving) state of the art, see [136].) Instead, only the final results (HHIs) are revealed. Local national supervisors would retain their current, typically extensive, authorities to access and examine the books and records of local institutions. Among other things, this protocol would leave them with the necessary capabilities and authorities in the event that the college's aggregate signal triggers a detailed local investigation.

The second issue concerns institutional confidentiality. As with financial stress indexes (Section 5.1), a concept along the lines of firm-level privacy makes sense. To take a concrete example, suppose that for each country pair and financial product category, the supervisory college should see monthly HHIs of cross-sectional concentrations (see below). An increasing HHI in a given cross-border market, coupled with similar exposure concentrations visible at the level of the college, might be evidence of growing imbalances worthy of closer scrutiny. We conjecture that HHIs can be computed with limited-precision, firm-level privacy guarantees. Work on differentially private statistical analysis supports that conjecture.

Finally, we expand on this example to describe a potential concrete computation: Consider the set of general collateral repurchase (GC repo) agreements. Each GC repo agreement represents a contract between two financial institutions and will have a notional amount measurable in U.S. dollars (USD).[35] Some subset of these GC repo contracts will cross borders (e.g., ABC Bank in New York contracts with XYZ bank in London). Define a given institution's market share in a particular cross-border GC repo market as the fraction of the notional values of contracts crossing the particular border and involving that institution. The HHI at any point in time is then the sum across firms of the squares of their market shares at that time. A higher HHI means greater concentration in the particular cross-border market.

For modest concentrations of exposure, a slightly modified version of this procedure will presumably not reveal sensitive aspects of individual firms' portfolios. Quantifying this statement is delicate, since this is an example in which firm-level differential privacy is impossible (it would not allow distinguishing between a setting in which one firm occupies a large fraction of the market and settings in which no single firm has a large share). In contrast, *limited-precision* differential privacy would be possible to provide, using, e.g., the smooth sensitivity framework or its variants [162, 53]. Whether the calculated confidence level is acceptable is a policy decision.[36] Given such a triggering signal, local national supervisors could pursue an attribution analysis and deeper investigation of the situation.[37]

[35] For GC repo, the notional amount would typically be identical to the principal balance being lent. Contracts denominated in other currencies can be converted to a USD notional using current exchange rates.

[36] Indeed, a HHI that reveals when a single institution has embedded an enormous position might even be regarded as a desirable policy outcome, as it might create endogenous market discipline. We emphasize that this example is chosen to illustrate the privacy protocol, not to suggest that it is the best measure of cross-border imbalances. The latter question is and should remain an active area for ongoing research. Other possible system-wide risk measures include aggregate leverage or aggregate margin-to-equity ratios [1, 74, 75].

[37]

6 Summary

The structure of information in financial markets creates incentives with pervasive effects on financial institutions and their relationships. Information asymmetries, incomplete contracts, and other inefficiencies can discourage market liquidity. In consequence, financial activity can be driven out of existence, or (more hopefully) into integrated firms where it is managed by corporate governance instead of contract enforcement. These same forces apply to supervisory institutions, which must balance the opposing demands of examination and disclosure. Examination can expose personally private data and strategic business information to examiners who must hold it in confidence to protect their supervisory relationship with the regulated entities, as well as to protect the interests of the firms and their customers. Disclosure works to reduce information asymmetries, empowering investors and fostering market discipline by better informing bond- and stockholders of commitments and risk exposures. This confidence/disclosure dichotomy tends to push supervisory information policies to one extreme or the other. We argue that in a number of intermediate cases, limited information sharing would be welfare-improving, improving inter-supervisor coordination, enhancing market discipline, and better informing investors, while still protecting important confidential and personal information. Indeed, we describe three illustrative usage scenarios where we believe beneficial intermediate solutions are available. These case studies all rely on recent tools in the fields of secure computation and statistical data privacy.

We acknowledge that we omit important aspects of the privacy problem from scope. For example, a religiously observant person might discuss faith if asked, but a mortgage loan officer in the U.S. is forbidden by the Equal Credit Opportunity Act from posing that question. The same borrower is likely quite reticent about sharing financial data, yet willingly submits to an intrusive financial investigation to get the loan. Financial economics provides an explanation for the latter behavior as a mechanism to alleviate asymmetries, but neither financial economics nor computer science is well positioned to address the former prohibition. That is better handled as an upshot of other historical, political, and social factors (see Bagby [10]). We take such rules as given and treat them as exogenous constraints on the problem.

We close with some general observations about data privacy and secure computation and suggest some areas for further research. Secure computation is widely agreed on as the formalism for addressing concerns that could be handled by an ideal trusted party. By providing a virtual trusted party beyond the control of any coalition of protocol participants, secure computation can avoid the need for a large pooled data repository. This solution mitigates several concerns that arise with the sharing of regulatory data. Most simply, a large pool is more exposed to security breaches. More subtly, legal restrictions may forbid a regulator from explicitly sharing data with another organization. Strategic considerations may similarly discourage such sharing. For example, legal protections accorded at the time of sharing may be altered by subsequent court decisions or legislative developments, such as the passage of the FOIA. At the same time, secure computation protocols present technical challenges. They are complex and not yet standardized in their implementation. Secure computation also presents a conceptual difficulty; the parties must agree on the computation (or set of computations) to be performed. For tasks like regulatory oversight, in which a human regulator's intuition may play a role in selecting what to inspect, specifying a computation may be challenging.

In contrast, no single formalism for reasoning about which computations to perform addresses all concerns. That is, we must still handle specific questions of data privacy—what to release and what to conceal—on a case-by-case basis. There are two main concerns with releasing financial data: individual privacy and institutional confidentiality. Individual privacy is best handled by formalisms along the lines of differential privacy. For most types of financial data, no single individual affects aggregate behavior significantly; given sufficient data, one can produce accurate statistical summaries. For example, for a public-use product generated from historical mortgage data, the principal concern is borrowers' confidentiality. Institutional confidentiality is more complicated. First, the cross-sectional dispersion in firm sizes makes it nearly impossible to hide all attributes of interest, while still preserving any reasonable statistical accuracy. Some institutions are so large—especially those we find most interesting—that there is no "crowd" for them to hide in. Second, as discussed in Section 2, certain aggregate statistics are public goods with the potential to improve coordination among firms, regulators, and investors. The most important example is the long-

standing publication of market prices to guide the invisible hand; other aggregates that are candidates for public disclosure are financial conditions indexes that may incorporate sensitive data. Although the public benefit of disclosure may outweigh the private harm, we argue that data privacy may frequently achieve much of the benefit of the aggregate signal, while still protecting sensitive facts. Rigorously formulating the public benefits of disclosure, and the way they trade off with confidentiality, remains important an research question.

A Some Major Laws Affecting Interagency Information Sharing

- Freedom of Information Act (5 U.S.C. 552)
- Privacy Act of 1974 (5 U.S.C. 552a)
- Right to Financial Privacy Act of 1978 (12 U.S.C. 3401)
- Home Mortgage Disclosure Act (12 U.S.C. 2801 et seq.)
- Dodd-Frank Act of 2010 (esp.: 12 USC 5321; 12 USC 5342)
  - Creates under Title I: Office of Financial Research
  - Creates under Title I: Financial Stability Oversight Council
- Gramm-Leach-Bliley Act of 1999 (esp.: 12 USC 5321; 12 USC 5342)
- Consumer Financial Protection Act of 2010, (12 U.S.C. 5481 et seq.)
- Bank Secrecy Act (31 USC 5311-5332)
- Trade Secrets Act (18 U.S.C. 1905; 18 U.S.C. 641)
- E-Government Act of 2002 (44 U.S.C. 101)
  - Includes as Title V: Confidential Information Protection and Statistical Efficiency Act of 2002
- Federal Information Security Management Act of 2002 (FISMA)
- Federal Records Act (44 U.S.C. 3101)
- Paperwork Reduction Act (44 U.S.C. 3510)

B Some Regulations Defining Sensitive Financial Regulatory Information

Text of these regulations is available in the Code of Federal Regulations (CFR), available online at: `http://www.law.cornell.edu/cfr/text/`. Individual sections of the CFR are typically available via appropriate refinement of the URL; for example, 12 CFR 792.11 is available at `http://www.law.cornell.edu/cfr/text/12/792.11`.

- Federal Reserve: 12 CFR 261.2(c)(1) defines "confidential supervisory information" (CSI). 12 CFR 268.205(a)(2)(i-iii) applies to alien employees and identifies three internal security classifications related specifically to CSI:
  - Restricted-Controlled FR: extremely sensitive information such as, "financial institution supervisory ratings and nonpublic advance information regarding bank mergers or failures."
  - Restricted FR: highly sensitive information such as, "single supervisory ratings (e.g., CAMELS, BOPEC, etc.), Federal Reserve examination and inspection reports and workpapers, Interagency Country Exposure Review Committee (ICERC) country exposure determinations, and shared national credit data or listings"
  - Internal FR: sensitive information such as, "foreign banking organization country studies and Federal Reserve risk assessments."

  It also defines three internal security classifications related to the implementation of monetary policy through the Federal Open Market Committee (FOMC):
  - Class I FOMC: extremely sensitive information such as, "the 'Bluebook,' drafts of meeting minutes, unreleased meeting transcripts, documents reflecting the preparation of semi-annual forecasts and related testimony, and certain sensitive internal memorandums and reports."
  - Class II FOMC: highly sensitive information such as, "Part I of the 'Greenbook,' reports of the Manager on domestic and foreign open market operations, and other materials on economic and financial developments"
  - Class III FOMC: sensitive information such as, "Part II of the Greenbook."
- CFPB: 12 CFR 1070.2(i)(1) and 12 CFR 1070.2(h). The latter is for Confidential Investigative Information (CII).
- OCC and OTS: 12 CFR 4.32(b). The OCC uses the term "Non-public OCC information" in lieu of CSI.
- FDIC: 12 CFR 309.5(g). The FDIC uses the concept of "exempt records" in lieu of CSI.
- FHFA: 12 CFR 1214 [proposed]. The FHFA has recently proposed a definition of "confidential supervisory information" that would apply to information prepared or received by the FHFA from Fannie Mae or Freddie Mac, the Federal Home Loan Banks, or the Office of Finance; [70]
- NCUA: 12 CFR 792.11(a). The NCUA uses the concept of "exempt records" in lieu of CSI.
- SEC: 17 CFR 230.122 and 17 CFR 200.83 and 17 CFR 230.406. The SEC conducts both examinations and investigations, the details of which generally may not be disclosed. However, information filed with the SEC outside of examinations and investigations may in general be further disclosed (e.g., under a FOIA request). Filers may request "confidential treatment" by following specific procedures.
- CFTC: 17 CFR 145.0. The CFTC distinguishes between "public records" and "nonpublic records," where the latter are simply any records not explicitly made public. Criteria under which the CFTC may decline to reveal nonpublic records are listed in 17 CFR 145.5. In addition, under 17 CFR 145.9, entities reporting to the CFTC may petition for "confidential treatment" of their submissions.

References

[1] E. Abbe, A. Khandani, and A. W. Lo. Privacy-preserving methods for sharing financial risk exposures. *American Economic Review*, 102(3):65–70, May 2012. URL http://www.aeaweb.org/articles.php?doi=10.1257/aer.102.3.65.

[2] N. R. Adam and J. C. Wortmann. Security-control methods for statistical databases: a comparative study. *ACM Computing Surveys*, 25(4), 1989.

[3] R. Agrawal and R. Srikant. Privacy-preserving data mining. In *SIGMOD*, volume 29(2), pages 439–450. ACM, 2000.

[4] G. A. Akerlof. The market for "lemons": Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 84(3):488–500, August 1970. ISSN 00335533. URL http://www.jstor.org/stable/1879431.

[5] D. Alford. Supervisory colleges: The global financial crisis and improving international supervisory coordination. *Emory International Law Review*, 24:57–82, 2010. URL http://www.law.emory.edu/fileadmin/journals/eilr/24/24.1/Alford.pdf.

[6] S. P. Anderson and R. Renault. Pricing, product diversity, and search costs: A bertrand-chamberlin-diamond model. *RAND Journal of Economics*, 30(4):719–735, Winter 1999. ISSN 07416261. URL http://www.jstor.org/stable/2556072.

[7] S. Arora, B. Barak, M. Brunnermeier, and R. Ge. Computational complexity and information asymmetry in financial products. *Communications of the ACM*, 54(5):101–107, May 2011. doi: 10.1145/1941487.1941511. URL http://portal.acm.org/citation.cfm?id=1941511.

[8] M. Avellaneda and R. Cont. Transparency in credit default swap markets. Technical report, Finance Concepts, July 2010. URL http://www.finance-concepts.com/en/finance-concepts-index.php?CatId=6.

[9] L. Backstrom, C. Dwork, and J. Kleinberg. Wherefore art thou r3579x? anonymized social networks, hidden patterns, and structural steganography. In *Proc. 16th Intl. World Wide Web Conference*, pages 181–190, 2007.

[10] J. W. Bagby. The public policy environment of the privacy-security conundrum/complement. In *Strategies and Policies in Digital Convergence*, chapter 12, pages 193–211. Idea Group Inc., 2007. URL http://faculty.ist.psu.edu/bagby/12.pdf.

[11] B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, and K. Talwar. Privacy, accuracy, and consistency too: a holistic solution to contingency table release. In *PODS*, pages 273–282. ACM, 2007.

[12] M. Barbaro and T. Zeller. A face is exposed for aol searcher no. 4417749. *The New York Times*, Aug. 2006.

[13] Basel Committee on Banking Supervision. Good practice principles on supervisory colleges. Technical report, BIS, October 2010. URL http://www.bis.org/publ/bcbs177.pdf.

[14] M. Bellare, V. T. Hoang, and P. Rogaway. Foundations of garbled circuits. In *ACM Conference on Computer and Communications Security*, pages 784–796, 2012.

[15] A. Ben-David, N. Nisan, and B. Pinkas. FairplayMP: a system for secure multi-party computation. In *ACM Conference on Computer and Communications Security*, pages 257–266, 2008.

[16] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for fault-tolerant distributed computing. In *Proc. 20th ACM Symp. on Theory of Computing*, pages 1–10, Chicago, 1988. ACM.

[17] G. Benston, M. Bromwich, R. Litan, and A. Wagenhofer. *Following the money: The Enron failure and the state of corporate disclosure*. Brookings Institution Press, 2003. URL http://books.google.com/books?id=GZs3CsJdSDkC&printsec=frontcover#v=onepage&q&f=false.

[18] R. Berner. Remarks of office of financial research (ofr) director richard berner at the joint conference of the federal reserve bank of cleveland and office of financial research, financial stability analysis: Using the tools, finding the data. Technical report, OFR, May 2013. URL http://www.treasury.gov/initiatives/ofr/news/Documents/Berner_speech_Cleveland_Fed_OFR_Conference_05-30-2013_FORMATTED.pdf.

[19] H. Bessembinder, W. Maxwell, and K. Venkataraman. Market transparency, liquidity externalities, and institutional trading costs in corporate bonds. *Journal of Financial Economics*, 82(2):251–288, September 2006. URL http://home.business.utah.edu/hank.bessembinder/publications/bondtransparency.pdf.

[20] R. Bhaskar, S. Laxman, A. Smith, and A. Thakurta. Discovering frequent patterns in sensitive data. In B. Rao, B. Krishnapuram, A. Tomkins, and Q. Yang, editors, *KDD*, pages 503–512. ACM, 2010. ISBN 978-1-4503-0055-1.

[21] R. Bhaskar, A. Bhowmick, V. Goyal, S. Laxman, and A. Thakurta. Noiseless database privacy. In D. H. Lee and X. Wang, editors, *ASIACRYPT*, volume 7073 of *Lecture Notes in Computer Science*, pages 215–232. Springer, 2011. ISBN 978-3-642-25384-3.

[22] A. V. Bhatia. Consolidated regulation and supervision in the united states. Technical report, IMF, 2011. URL http://www.imf.org/external/pubs/cat/longres.aspx?sk=24607.0.

[23] B. Biais, P. Hillion, and C. Spatt. Price discovery and learning during the preopening period in the paris bourse. *Journal of Political Economy*, 107(6):1218–1248, December 1999. ISSN 00223808. URL http://www.jstor.org/stable/10.1086/250095.

[24] M. Bishop. *Computer Security: Art and Science*. Addison-Wesley, 2002.

[25] A. Blum, C. Dwork, F. McSherry, and K. Nissim. Practical Privacy: The SuLQ Framework. In *PODS*, pages 128–138. ACM, 2005.

[26] Board of Governors of the Federal Reserve. Supervisory letter sr 00-13: Framework for financial holding company supervision. Technical report, Federal Reserve Board, August 2000. URL http://www.federalreserve.gov/boarddocs/srletters/2000/sr0013.htm.

[27] Board of Governors of the Federal Reserve. Reporting forms: Fr y-14m, capital assessments and stress testing. Technical report, Federal Reserve, October 2012. URL http://www.federalreserve.gov/apps/reportforms/reporthistory.aspx?sOoYJ+5BzDYnbIw+U9pka3sMtCMopzoV.

[28] Board of Governors of the Federal Reserve. Reporting forms. Technical report, Federal Reserve, April 2013. URL http://www.federalreserve.gov/apps/reportforms/default.aspx. Internet resource, accessed April 28, 2013.

[29] E. Boehmer, G. Saar, and L. Yu. Lifting the veil: An analysis of pre-trade transparency at the nyse. *Journal of Finance*, 60(2):783–815, April 2005. ISSN 00221082. URL http://www.jstor.org/stable/3694767.

[30] D. Bogdanov, R. Talviste, and J. Willemson. Deploying secure multi-party computation for financial data analysis. Technical report, 2013.

[31] P. Bogetoft, I. Damgård, T. Jokobsen, K. Nielsen, J. Pagter, and T. Toft. A practical implementation of secure auctions based on multiparty integer computation. *Financial Cryptography and Data Security*, 4107:142–147, 2006. URL http://link.springer.com/chapter/10.1007/11889663_10.

[32] P. Bogetoft, K. Boye, H. Neergaard-Petersen, and K. Nielsen. Reallocating sugar beet contracts: Can sugar production survive in denmark? *European Review of Agricultural Economics*, 34, 2007.

[33] P. Bogetoft, D. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. Nielsen, J. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft. Secure multiparty computation goes live. In *Financial Cryptography*, volume 5628 of *LNCS*, pages 325–343. Springer-Verlag, 2009. Available at http://eprint.iacr.org/2008/068.

[34] L. D. Brandeis. *Other People's Money: And How the Bankers Use It*. Frederick A. Stokes Company, 1914. URL http://www.law.louisville.edu/library/collections/brandeis/node/196.

[35] M. K. Brunnermeier. *Asset Pricing under Asymmetric Information: Bubbles, Crashes, Technical Analysis, and Herding: Bubbles, Crashes, Technical Analysis, and Herding*. Oxford U. Press, 2001.

[36] R. J. Caballero and A. Krishnamurthy. Collective risk management in a flight to quality episode. *Journal of Finance*, 63(5):2195–2230, 2008. URL http://www.jstor.org/stable/10.2307/i25094500.

[37] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proc. 20th ACM Symp. on Theory of Computing*, pages 11–19, Chicago, 1988. ACM.

[38] Y. Chen, S. Chong, I. A. Kash, T. Moran, and S. P. Vadhan. Truthful mechanisms for agents that value privacy. *CoRR*, abs/1111.5472, 2011.

[39] Common Data Project. Private mapmaker v0.2, 2011. URL http://blog.myplaceinthecrowd.org/2011/04/27/the-cdp-private-map-maker-v0-2/.

[40] Consumer Financial Protection Bureau. Federal housing finance agency and consumer financial protection bureau to partner on development of national mortgage database. Technical report, CFPB, November 2012. URL http://www.consumerfinance.gov/pressreleases/federal-housing-finance-agency-and-consumer-financial-protection-bureau-to-partner-on-development-of-national-mortgage-database/.

[41] S. Coull, C. Wright, F. Monrose, A. Keromytis, and M. Reiter. Taming the devil: Techniques for evaluating anonymized network data. In *15th Annual Network & Distributed System Security Symposium (NDSS)*, 2008.

[42] J. Coval, J. Jurek, and E. Stafford. The economics of structured finance. *Journal of Economic Perspectives*, 23 (1):3–25, Winter 2009. URL http://www.aeaweb.org/articles.php?doi=10.1257/jep.23.1.

[43] E. Dal B. Regulatory capture: A review. *Oxford Review of Economic Policy*, 22(2):203–225, Summer 2006. URL http://red.ap.teacup.com/inouekoji/html/regulatory_capture_published.pdf.

[44] I. Damgård, M. Keller, E. Larraia, C. Miles, and N. P. Smart. Implementing AES via an actively/covertly secure dishonest-majority mpc protocol. In *SCN*, pages 241–263, 2012.

[45] T. V. Dang, G. Gorton, and B. Holmstrm. Opacity and the optimality of debt for liquidity provision. Working paper, Yale University, November 2009. URL http://www.econ.yale.edu/~dirkb/teach/pdf/d/dang/Paper_Liquidity.pdf.

[46] A. De. Lower Bounds in Differential Privacy. In *TCC*, pages 321–338, 2012.

[47] Department of Justice. Exemption 8. In *Guide to the Freedom of Information Act*. 2009. URL http://www.justice.gov/oip/foia_guide09/exemption8.pdf.

[48] I. Dinur and K. Nissim. Revealing Information While Preserving Privacy. In *PODS*, pages 202–210. ACM, 2003.

[49] G. T. Duncan and S. Mukherjee. Optimal disclosure limitation strategy in statistical databases: Deterring tracker attacks through additive noise. *Journal of the American Statistical Association*, 95(451):720–729, September 2000. ISSN 01621459. URL http://www.jstor.org/stable/2669452.

[50] C. Dwork. Differential Privacy. In *ICALP*, LNCS, pages 1–12. Springer, 2006.

[51] C. Dwork. Differential privacy: A survey of results. In *TAMC*, pages 1–19. Springer, 2008.

[52] C. Dwork. The differential privacy frontier. In *TCC*, pages 496–502. Springer, 2009.

[53] C. Dwork and J. Lei. Differential Privacy and Robust Statistics. In *STOC*, pages 371–380, 2009.

[54] C. Dwork and M. Naor. On the difficulties of disclosure prevention in statistical databases or the case for differential privacy. *J. Privacy and Confidentiality*, 2(1), 2010.

[55] C. Dwork and K. Nissim. Privacy-preserving datamining on vertically partitioned databases. In *CRYPTO*, LNCS, pages 528–544. Springer, 2004.

[56] C. Dwork and A. Roth. The algorithmic foundations of differential privacy. To appear, 2013.

[57] C. Dwork and A. Smith. Differential privacy for statistics: What we know and what we want to learn. *J. Privacy and Confidentiality*, 1(2), 2009.

[58] C. Dwork and S. Yekhanin. New efficient attacks on statistical disclosure control mechanisms. In *CRYPTO*, pages 469–480. Springer, 2008.

[59] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor. Our Data, Ourselves: Privacy Via Distributed Noise Generation. In *EUROCRYPT*, LNCS, pages 486–503. Springer, 2006.

[60] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *TCC*, LNCS, pages 265–284. Springer, 2006.

[61] C. Dwork, F. McSherry, and K. Talwar. The price of privacy and the limits of LP decoding. In *STOC*, pages 85–94. ACM, 2007. ISBN 978-1-59593-631-8.

[62] D. J. Elliott, G. Feldberg, and A. Lehnert. The history of cyclical macroprudential policy in the united states. OFR Working Paper 0008, Office of Financial Research, May 2013. URL `http://www.treasury.gov/initiatives/ofr/research/Documents/OFRwp0008_ElliottFeldbergLehnert_AmericanCyclicalMacroprudentialPolicy.pdf`.

[63] E. J. Elton, M. J. Gruber, and J. A. Busse. Are investors rational? choices among index funds. *Journal of Finance*, 59(1):261–288, February 2004. ISSN 00221082. URL `http://www.jstor.org/stable/3694896`.

[64] A. Evfimievski, J. Gehrke, and R. Srikant. Limiting privacy breaches in privacy preserving data mining. In *PODS*, pages 211–222. ACM, 2003. ISBN 1-58113-670-6.

[65] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. Common knowledge revisited. *Annals of Pure and Applied Logic*, 96(1):89–105, 1999. URL `http://arxiv.org/pdf/cs.LO/9809003.pdf`.

[66] B. Faltings, K. Leyton-Brown, and P. Ipeirotis, editors. *ACM Conference on Electronic Commerce, EC '12, Valencia, Spain, June 4-8, 2012*, 2012. ACM. ISBN 978-1-4503-1415-2.

[67] E. F. Fama. Efficient capital markets: A review of theory and empirical work. *Journal of Finance*, 25(2):383–417, 1970. URL `http://onlinelibrary.wiley.com/doi/10.1111/j.1540-6261.1970.tb00518.x/abstract`.

[68] E. F. Fama. *Foundations of Finance: Portfolio Decisions and Securities Prices*. Basic Books, 1976.

[69] Federal Committee on Statistical Methodology. Statistical policy working paper 22 (revised 2005)—report on statistical disclosure limitation methodology. `http://www.fcsm.gov/working-papers/spwp22.html`, 2006.

[70] Federal Housing Finance Agency. Availability of non-public information. Proposed Rule RIN 2590AA06, FHFA, January 2013. URL `http://www.gpo.gov/fdsys/pkg/FR-2013-01-29/pdf/2013-01427.pdf`.

[71] R. J. Feldman and J. Schmidt. Post-crisis use of financial market data in bank supervision. *Annual Report of the Federal Reserve Bank of Minneapolis*, 2011:4–41, October 2012. URL `http://www.minneapolisfed.org/publications_papers/issue.cfm?id=365`.

[72] Financial Crisis Inquiry Commission. *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*. U.S. Government Printing Office, 2011. URL `http://fcic.law.stanford.edu/report`.

[73] Financial Stability Board. Enhancing the risk disclosures of banks: Report of the enhanced disclosure task force. Edtf report, Financial Stability Board, October 2012. URL `http://www.financialstabilityboard.org/publications/r_121029.pdf`.

[74] Financial Stability Board and International Monetary Fund. The financial crisis and information gaps: Report to the g-20 finance ministers and central bank governors. Technical report, Financial Stability Board, October 2009. URL http://www.financialstabilityboard.org/publications/r_091107e.pdf.

[75] Financial Stability Board and International Monetary Fund. The financial crisis and information gaps: Progress report: Action plans and timetables. Technical report, Financial Stability Board, May 2010. URL http://www.imf.org/external/np/g20/pdf/053110.pdf.

[76] Financial Stability Board and International Monetary Fund. The financial crisis and information gaps: Implementation progress report. Technical report, Financial Stability Board, June 2011. URL http://www.imf.org/external/np/g20/pdf/063011.pdf.

[77] Financial Stability Board and International Monetary Fund. The financial crisis and information gaps: Progress report on the g-20 data gaps initiative: Status, action plans, and timetables. Technical report, Financial Stability Board, September 2012. URL http://www.imf.org/external/np/g20/pdf/093012.pdf.

[78] L. Fleischer and Y.-H. Lyu. Approximately optimal auctions for selling privacy when costs are correlated with data. In Faltings et al. [66], pages 568–585. ISBN 978-1-4503-1415-2.

[79] M. D. Flood. Deposit insurance problems and solutions. *Federal Reserve Bank of St. Louis Review*, 93(1):28–33, January-February 1993. URL http://research.stlouisfed.org/publications/review/93/01/Flood_Jan_Feb1993.pdf.

[80] T. K. Frederiksen and J. B. Nielsen. Fast and maliciously secure two-party computation using the gpu. Cryptology ePrint Archive, Report 2013/046, 2013. http://eprint.iacr.org/.

[81] T. K. Frederiksen, T. P. Jakobsen, J. B. Nielsen, P. S. Nordholt, and C. Orlandi. Minilego: Efficient secure two-party computation from general assumptions. In Johansson and Nguyen [117], pages 537–556. ISBN 978-3-642-38347-2, 978-3-642-38348-9.

[82] G. Fries. Disclosure review and the 2001 survey of consumer finances. Technical report, Federal Reserve Board, August 2003. URL http://www.federalreserve.gov/econresdata/scf/files/asa2003f6.pdf.

[83] A. Fung, M. Graham, and D. Weil. *Full Disclosure: The Perils and Promise of Transparency*. Cambridge University Press, 2008. URL http://www.cambridge.org/gb/knowledge/isbn/item1164221/?site_locale=en_GB.

[84] S. R. Ganta, S. P. Kasiviswanathan, and A. Smith. Composition attacks and auxiliary information in data privacy. In *KDD '08: Proceeding of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 265–273. ACM, 2008.

[85] J. Geanakoplos. Common knowledge. *Journal of Economic Perspectives*, 6(4):53–82, Autumn 1992. ISSN 08953309. URL http://www.jstor.org/stable/2138269.

[86] J. Geanakoplos. Common knowledge. In R. Aumann and S. Hart, editors, *Handbook of Game Theory, Volume 2*, chapter 40, pages 1437–1496. Elsevier Science, 1994. URL http://classes.maxwell.syr.edu/ecn611/Geanakoplos2.pdf.

[87] J. Geanakoplos. The arrow-debreu model of general equilibrium. Technical report, Yale U., 2004. URL http://cowles.econ.yale.edu/P/cp/p10b/p1090.pdf.

[88] J. Gehrke, E. Lui, and R. Pass. Towards privacy for social networks: A zero-knowledge based definition of privacy. In Y. Ishai, editor, *TCC*, volume 6597 of *Lecture Notes in Computer Science*, pages 432–449. Springer, 2011. ISBN 978-3-642-19570-9.

[89] J. Gehrke, M. Hay, E. Lui, and R. Pass. Crowd-blending privacy. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO*, volume 7417 of *Lecture Notes in Computer Science*, pages 479–496. Springer, 2012. ISBN 978-3-642-32008-8.

[90] General Accounting Office. Better information sharing among financial services regulators could improve protections for consumers. Technical Report GAO-04-882R, United States General Accounting Office, June 2004. URL http://www.gpo.gov/fdsys/pkg/GAOREPORTS-GAO-04-882R/content-detail.html.

[91] Georgetown Law Library. Freedom of information act (federal) - research guide. Technical report, Georegetown U., 2013. URL http://www.law.georgetown.edu/library/research/guides/foia.cfm.

[92] A. Ghosh and A. Roth. Selling privacy at auction. In Y. Shoham, Y. Chen, and T. Roughgarden, editors, *ACM Conference on Electronic Commerce*, pages 199–208. ACM, 2011. ISBN 978-1-4503-0261-6. arxiv:1011.1375.

[93] O. Goldreich. *Foundations of Cryptography*, volume Basic Tools. Cambridge University Press, 2001.

[94] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In A. V. Aho, editor, *STOC*, pages 218–229. ACM, 1987. ISBN 0-89791-221-7.

[95] D. Gollmann. *Computer Security*. Wiley, third edition, 2011.

[96] S. D. Gordon, T. Malkin, M. Rosulek, and H. Wee. Multi-party computation of polynomials and branching programs without simultaneous interaction. In Johansson and Nguyen [117], pages 575–591. ISBN 978-3-642-38347-2, 978-3-642-38348-9.

[97] G. B. Gorton. The panic of 2007. Working Paper 14358, NBER, 2008. URL http://www.nber.org/papers/w14358.

[98] Government Accountability Office. Information security: Protecting personally identifiable information. GAO Report to Congressional Requesters GAO-08-343, GAO, January 2008. URL http://www.gao.gov/new.items/d08343.pdf.

[99] J. Gray. Notes on data base operating systems. In G. Goos and J. Hartmanis, editors, *Operating Systems: An Advanced Course*. Springer Verlag, 1978.

[100] S. J. Grossman and J. E. Stiglitz. On the impossibility of informationally efficient markets. *American Economic Review*, 70(3):393–408, June 1980. URL http://www.jstor.org/stable/10.2307/1805228.

[101] M. Gymrek, A. L. McGuire, D. Golan, E. Halperin, and Y. Erlich. Identifying personal genomes by surname inference. *Science*, 339(6117):321–324, January 2013.

[102] R. Hall, L. Wasserman, and A. Rinaldo. Random differential privacy. *J. Privacy and Confidentiality*, 4(2), 2012.

[103] M. Hardt, K. Ligett, and F. McSherry. A simple and practical algorithm for differentially private data release. In P. L. Bartlett, F. C. N. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, editors, *NIPS*, pages 2348–2356, 2012.

[104] S. Hawala, L. Zayatz, and S. Rowland. American factfinder: Disclosure limitation for the advanced query system. *Journal of Official Statistics, Stockholm*, 20(1):115–124, 2004. URL http://www.census.gov/srd/sdc/AdvancedQuerySystem.pdf.

[105] T. Hendershott and C. M. Jones. Island goes dark: Transparency, fragmentation, and regulation. *Review of Financial Studies*, 18(3):743–793, Autumn 2005. ISSN 08939454. URL http://www.jstor.org/stable/3598078.

[106] W. Henecka, S. Kögl, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg. TASTY: tool for automating secure two-party computations. In *ACM Conference on Computer and Communications Security*, pages 451–462, 2010.

[107] B. Holmström. The nature of liquidity provision: When ignorance is bliss. Presidential Address, 2012. URL http://www.youtube.com/watch?feature=player_embedded&v=4yQO512B-_A.

[108] N. Homer, S. Szelinger, M. Redman, D. Duggan, W. Tembe, J. Muehling, J. V. Pearson, D. A. Stephan, , S. F. Nelson, and D. W. Craig. Resolving individuals contributing trace amounts of dna to highly complex mixtures using high-density snp genotyping microarrays. *PLOS Genetics*, 4(8), 2008.

[109] A. Hortaçsu and C. Syverson. Product differentiation, search costs, and competition in the mutual fund industry: A case study of s&p 500 index funds. *Quarterly Journal of Economics*, 119(2):403–456, May 2004. ISSN 00335533. URL `http://www.jstor.org/stable/25098690`.

[110] Y. Huang, D. Evans, J. Katz, and L. Malka. Faster secure two-party computation using garbled circuits. In *USENIX Security Symposium*, 2011.

[111] Y. Huang, J. Katz, and D. Evans. Quid-pro-quo-tocols: Strengthening semi-honest protocols with dual execution. In *IEEE Symposium on Security and Privacy*, pages 272–284, 2012.

[112] Z. Huang and S. Kannan. The exponential mechanism for social welfare: Private, truthful, and nearly optimal. In *FOCS*, pages 140–149. IEEE Computer Society, 2012. ISBN 978-1-4673-4383-1.

[113] M. Illing and Y. Liu. Measuring financial stress in a developed country: An application to canada. *Journal of Financial Stability*, 2(3):243–265, October 2006. URL `http://www.sciencedirect.com/science/article/pii/S1572308906000301`.

[114] International Organization of Securities Commissions. Issues raised by dark liquidity. Consultation Report CR05/10, IOSCO, October 2010. URL `http://www.iosco.org/library/pubdocs/pdf/IOSCOPD336.pdf`.

[115] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. Cryptography with constant computational overhead. In *STOC*, pages 433–442, 2008.

[116] Y. Ishai, M. Prabhakaran, and A. Sahai. Founding cryptography on oblivious transfer - efficiently. In *CRYPTO*, pages 572–591, 2008.

[117] T. Johansson and P. Q. Nguyen, editors. *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, 2013. Springer. ISBN 978-3-642-38347-2, 978-3-642-38348-9.

[118] E. Kane. The inevitability of shadowy banking. Technical report, Boston College, 2012. URL `http://www.frbatlanta.org/documents/news/conferences/12fmc/12fmc_kane.pdf`.

[119] S. P. Kasiviswanathan and A. Smith. A note on differential privacy: Defining resistance to arbitrary side information. *CoRR*, arXiv:0803.39461 [cs.CR], 2008.

[120] S. P. Kasiviswanathan, M. Rudelson, A. Smith, and J. Ullman. The price of privately releasing contingency tables and the spectra of random matrices with correlated rows. In L. J. Schulman, editor, *STOC*, pages 775–784. ACM, 2010. ISBN 978-1-4503-0050-6.

[121] S. P. Kasiviswanathan, M. Rudelson, and A. Smith. The power of linear reconstruction attacks. In *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2013.

[122] J. Katz and Y. Lindell. *Introduction to Modern Cryptography: Principles and Protocols*. Chapman & Hall, 2007.

[123] M. Kearns, M. M. Pai, A. Roth, and J. Ullman. Mechanism design in large games: Incentives and privacy. *CoRR*, abs/1207.4084, 2012.

[124] R. W. Kenney and B. Klein. The economics of block booking. *Journal of Law and Economics*, 26(3):497–540, October 1983. ISSN 00222186. URL `http://www.jstor.org/stable/725036`.

[125] A. B. Kennickell and J. Lane. Measuring the impact of data protection techniques on data utility: Evidence from the survey of consumer finances. In *PSD'06 Proceedings of the 2006 CENEX-SDC project international conference on Privacy in Statistical Databases*, pages 291–303, 2006. URL `http://dl.acm.org/citation.cfm?id=2173112`.

[126] K. Kenthapadi, N. Mishra, and K. Nissim. Simulatable auditing. In *PODS*, 2005.

[127] D. Kifer and A. Machanavajjhala. No Free Lunch in Data Privacy. In *SIGMOD*, pages 193–204, 2011.

[128] D. Kifer and A. Machanavajjhala. A rigorous and customizable framework for privacy. In M. Benedikt, M. Krötzsch, and M. Lenzerini, editors, *PODS*, pages 77–88. ACM, 2012. ISBN 978-1-4503-1248-6.

[129] V. Kolesnikov and T. Schneider. Improved garbled circuit: Free XOR gates and applications. In *ICALP (2)*, pages 486–498, 2008.

[130] A. Komai and G. Richardson. A brief history of regulations regarding financial markets in the united states: 1789. In M. Brose, M. Flood, D. Krishna, and W. Nichols, editors, *Handbook of Financial Data and Risk Information, Vol. I*. Cambridge University Press, 2013. URL `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1932574#`.

[131] S. P. Kothari, S. Shu, and P. D. Wysocki. Do managers withhold bad news? *Journal of Accounting Research*, 47(1):241–276, March 2009. URL `http://web.mit.edu/wysockip/www/papers/KSW2008.pdf`.

[132] B. Kreuter, shelat abhi, and C. Shen. Billion-gate secure computation with malicious adversaries. USENIX Security. Available at Cryptology ePrint Archive, Report 2012/179, 2012. `http://eprint.iacr.org/`.

[133] J.-J. Laffont and J. Tirole. The politics of government decision-making: A theory of regulatory capture. *Quarterly Journal of Economics*, 106(4):1089–1127, November 1991. ISSN 00335533. URL `http://www.jstor.org/stable/2937958`.

[134] J. Lewellen and J. Shanken. Learning, asset-pricing tests, and market efficiency. *Journal of Finance*, 57(3): 1113–1145, 2002. URL `http://onlinelibrary.wiley.com/doi/10.1111/1540-6261.00456/abstract`.

[135] K. Ligett and A. Roth. Take it or leave it: Running a survey when privacy comes at a cost. In P. W. Goldberg, editor, *WINE*, volume 7695 of *Lecture Notes in Computer Science*, pages 378–391. Springer, 2012. ISBN 978-3-642-35310-9. arxiv:1202.4741.

[136] Y. Lindell. Efficient secure computation at tcc 2013. In *MPC Lounge Blog (Online)*, March 3 2013. `http://mpclounge.wordpress.com`.

[137] Y. Lindell and B. Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. In *EUROCRYPT*, pages 52–78, 2007.

[138] Y. Lindell and B. Pinkas. Secure multiparty computation for privacy-preserving data mining. *Journal of Privacy and Confidentiality*, 1(1), 2009.

[139] Y. Lindell and B. Pinkas. Secure two-party computation via cut-and-choose oblivious transfer. In *TCC*, pages 329–346, 2011.

[140] Y. Lindell, B. Pinkas, and N. P. Smart. Implementing two-party computation efficiently with security against malicious adversaries. In *SCN*, pages 2–20, 2008.

[141] Y. Lindell, E. Oxman, and B. Pinkas. The IPS compiler: Optimizations, variants and concrete efficiency. In *CRYPTO*, pages 259–276, 2011.

[142] A. Machanavajjhala, D. Kifer, J. M. Abowd, J. Gehrke, and L. Vilhuber. Privacy: Theory meets practice on the map. In *24th International Conference on Data Engineering (ICDE)*, pages 277–286. IEEE, 2008.

[143] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella. Fairplay - secure two-party computation system. In *USENIX Security Symposium*, pages 287–302, 2004.

[144] E. McCallister, T. Grance, and K. Scarfone. Guide to protecting the confidentiality of personally identifiable information (pii): Recommendations of the national institute of standards and technology. NIST Special Publication 800-122, National Institute of Standards and Technology, April 2010. URL `http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf`.

[145] R. H. McGuckin and S. V. Nguyen. Public use microdata: Disclosure and usefulness. Discussion Papers, Center for Economic Studies CES 88-3, U.S. Bureau of the Census, September 1988. URL https://www.ces.census.gov/docs/cache/paper_contents_100109.pdf.

[146] J. McNabb, D. Timmons, J. Song, and C. Puckett. Uses of administrative data at the social security administration. *Social Security Bulletin*, 69(1):75–84, 2009. URL http://www.socialsecurity.gov/policy/docs/ssb/v69n1/v69n1p75.pdf.

[147] F. McSherry and R. Mahajan. Differentially-private network trace analysis. In S. Kalyanaraman, V. N. Padmanabhan, K. K. Ramakrishnan, R. Shorey, and G. M. Voelker, editors, *SIGCOMM*, pages 123–134. ACM, 2010. ISBN 978-1-4503-0201-2.

[148] F. McSherry and I. Mironov. Differentially Private Recommender Systems: Building Privacy into the Net. In *KDD*, pages 627–636. ACM New York, NY, USA, 2009.

[149] F. McSherry and K. Talwar. Mechanism design via differential privacy. In *FOCS*, pages 94–103. IEEE, 2007.

[150] R. C. Merton. On the pricing of contingent claims and the modigliani-miller theorem. *Journal of Financial Economics*, 5(2):241–249, November 1977. ISSN 00223808. URL http://www.sciencedirect.com/science/article/pii/0304405X77900204.

[151] E. Meyer. Financing agriculture. Technical report, War Finance Corporation, October 1922. URL http://archive.org/details/financingagricu00meye. Address of Eugene Meyer, Jr. before the State Bank Division of the American Bankers Association, New York, October 2, 1922.

[152] P. Milgrom and J. Roberts. Bargaining costs, influence costs, and the organization of economic activity. In J. E. Alt and K. A. Shepsle, editors, *Perspectives on Positive Political Economy*, chapter 3, pages 57–89. Cambridge University Press, 1990. URL http://www.stanford.edu/~milgrom/publishedarticles/BargainingCosts.pdf.

[153] P. Milgrom and N. Stokey. Information, trade and common knowledge. *Journal of Economic Theory*, 26(1): 17–27, February 1982. URL http://www.sciencedirect.com/science/article/pii/0022053182900461.

[154] P. Mohassel and S. S. Sadeghian. How to hide circuits in mpc an efficient framework for private function evaluation. In Johansson and Nguyen [117], pages 557–574. ISBN 978-3-642-38347-2, 978-3-642-38348-9.

[155] A. Narayanan and V. Shmatikov. Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset). *University of Texas at Austin*, 2008.

[156] A. Narayanan and V. Shmatikov. De-anonymizing social networks. In *IEEE Symp. Security and Privacy*, pages 173–187, 2009.

[157] A. Narayanan and V. Shmatikov. Myths and fallacies of "personally identifiable information". *Commun. ACM*, 53(6):24–26, 2010.

[158] A. Narayanan, E. Shi, and B. I. P. Rubinstein. Link prediction by de-anonymization: How we won the kaggle social network challenge. In *IJCNN*, pages 1825–1834. IEEE, 2011. ISBN 978-1-4244-9635-8.

[159] National Opinion Research Center (NORC). Confidentiality pledge. Technical report, NORC, 2013. URL http://scf.norc.org/confidentiality.html. Downloaded 7 June 2013.

[160] J. B. Nielsen and C. Orlandi. LEGO for two-party secure computation. In *TCC*, pages 368–386, 2009.

[161] J. B. Nielsen, P. S. Nordholt, C. Orlandi, and S. S. Burra. A new approach to practical active-secure two-party computation. In *CRYPTO*, pages 681–700, 2012.

[162] K. Nissim, S. Raskhodnikova, and A. Smith. Smooth sensitivity and sampling in private data analysis. In *Symp. Theory of Computing (STOC)*, pages 75–84. ACM, 2007. Full paper: http://www.cse.psu.edu/~asmith/pubs/NRS07.

[163] K. Nissim, C. Orlandi, and R. Smorodinsky. Privacy-aware mechanism design. In Faltings et al. [66], pages 774–789. ISBN 978-1-4503-1415-2. arxiv:1111.3350.

[164] K. Nissim, R. Smorodinsky, and M. Tennenholtz. Approximately optimal mechanism design via differential privacy. In S. Goldwasser, editor, *ITCS*, pages 203–213. ACM, 2012. ISBN 978-1-4503-1115-1. arxiv:1004.2888.

[165] B. Obama. Executive order 13526 of december 29, 2009: Classified national security information. *Federal Register*, 75(2):707–731, January 2010. URL `http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31418.pdf#page=3`. Tuesday, January 5, 2010.

[166] M. V. Oet, T. Bianco, D. Gramlich, and S. J. Ong. Safe: An early warning system for systemic banking risk. Working Paper 11-29, Federal Reserve Bank of Cleveland, 2011. URL `http://www.clevelandfed.org/research/workpaper/2011/wp1129.pdf`.

[167] M. V. Oet, R. Eiben, T. Bianco, D. Gramlich, and S. J. Ong. The financial stress index: Identification of systemic risk conditions. Working Paper 11-30, Federal Reserve Bank of Cleveland, 2011. URL `http://www.clevelandfed.org/research/data/financial_stress_index/about.cfm`.

[168] M. V. Oet, T. Bianco, D. Gramlich, and S. J. Ong. Financial stress index: A lens for supervising the financial system. Working Paper 12-37, Federal Reserve Bank of Cleveland, 2012. URL `http://www.clevelandfed.org/research/workpaper/2012/wp1237.pdf`.

[169] Office of Financial Research. Annual report. Technical report, OFR, 2012.

[170] Office of Management and Budget. Implementation guidance for title v of the e-government act, confidential information protection and statistical efficiency act of 2002 (cipsea). *Federal Register*, 72(115):33362–33377, June 2007. URL `http://www.gpo.gov/fdsys/granule/FR-2007-06-15/E7-11542/content-detail.html`.

[171] M. M. Pai and A. Roth. Privacy and mechanism design. *SIGECOM Exchange*, 2013.

[172] R. Payne. Informed trade in spot foreign exchange markets: an empirical investigation. *Journal of International Economics*, 61(2):307329, December 2003. URL `http://www.sciencedirect.com/science/article/pii/S0022199603000035`.

[173] S. Peristiani, D. P. Morgan, and V. Savino. The information value of the stress test and bank opacity. Staff Report 460, FRB of New York, July 2010. URL `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1650670`.

[174] S. Pianalto. Financial stability: Lessons from monetary policy. Technical report, Federal Reserve Bank of Cleveland, May 2013. URL `http://www.clevelandfed.org/for_the_public/news_and_media/speeches/2013/pianalto_20130531.cfm`. Speech delivered at Cleveland Fed and OFR Conference on Financial Stability Analysis, Board of Governors of the Federal Reserve System, Washington, D.C, May 31, 2013.

[175] B. Pinkas, T. Schneider, N. P. Smart, and S. C. Williams. Secure two-party computation is practical. In *ASIACRYPT*, pages 250–267, 2009.

[176] Public Interest Declassification Board. Improving declassification: A report to the president from the public interest declassification board. Technical report, Public Interest Declassification Board, December 2007. URL `http://www.archives.gov/declassification/pidb/improving-declassification.pdf`.

[177] M. Qi. Exposure at default of unsecured credit cards. OCC Economics Working Paper 2009-2, OCC, July 2009. URL `http://www.occ.gov/publications/publications-by-type/economics-working-papers/2013-2009/wp2009-2.pdf`.

[178] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In D. S. Johnson, editor, *Proceedings of the 21st annual ACM Symposium on Theory of Computing (STOC'89)*, pages 73–85. ACM, 1989.

[179] B. F. Ribeiro, W. Chen, G. Miklau, and D. F. Towsley. Analyzing privacy in enterprise packet trace anonymization. In *NDSS*. The Internet Society, 2008.

[180] A. Roth. The algorithmic foundations of data privacy (lecture notes). http://www.cis.upenn.edu/~aaroth/courses/privacyF11.html, 2011.

[181] A. Roth and G. Schoenebeck. Conducting truthful surveys, cheaply. In Faltings et al. [66], pages 826–843. ISBN 978-1-4503-1415-2. arxiv:1203.0353.

[182] A. Rubinstein and A. Wolinsky. Decentralized trading, strategic behaviour and the walrasian outcome. *Review of Economic Studies*, 57(1):pp. 63–78, January 1990. ISSN 00346527. URL http://www.jstor.org/stable/2297543.

[183] M. L. Schapiro. Testimony concerning the lehman brothers examiner's report by chairman mary l. schapiro, u.s. securities and exchange commission, before the house financial services committee. Technical report, SEC, 2010. URL http://www.sec.gov/news/testimony/2010/ts042010mls.htm.

[184] B. Schoenmakers and P. Tuyls. Practical two-party computation based on the conditional gate. In *ASIACRYPT*, pages 119–136, 2004.

[185] Securities and Exchange Commission. Selective disclosure and insider trading. Technical Report Release 33-7881, SEC, 2000. URL https://www.sec.gov/rules/final/33-7881.htm.

[186] Securities and Exchange Commission. Compliance and disclosure interpretations: Exchange act rules. Technical report, SEC, 2012. URL http://www.sec.gov/divisions/corpfin/guidance/exchangeactrules-interps.htm.

[187] Securities and Exchange Commission. Securities and exchange commission forms list. Technical report, SEC, April 2013. URL http://www.sec.gov/about/forms/secforms.htm. Internet resource, accessed April 28, 2013.

[188] A. Shelat. Personal communication.

[189] shelat abhi and C.-H. Shen. Two-output secure computation with malicious adversaries. In *EUROCRYPT*, pages 386–405, 2011.

[190] M. Srivatsa and M. Hicks. Deanonymizing mobility traces: using social network as a side-channel. In T. Yu, G. Danezis, and V. D. Gligor, editors, *ACM Conference on Computer and Communications Security*, pages 628–637. ACM, 2012. ISBN 978-1-4503-1651-4.

[191] J. E. Stiglitz. The contributions of the economics of information to twentieth century economics. *Quarterly Journal of Economics*, 115(4):1441–1478, November 2000. URL http://www.jstor.org/stable/10.2307/2586930.

[192] R. Strausz. Honest certification and the threat of capture. *International Journal of Industrial Organization*, 23(1):45–62, 2005. URL http://www.sciencedirect.com/science/article/pii/S0167718704001092.

[193] R. Sullivan. Us bond market rallies after downgrade. Technical report, Financial Times, August 2011. August 14, 2011 12:36 pm.

[194] L. Sweeney. *Computational Disclosure Control: A Primer on Data Privacy Protection*. PhD thesis, MIT, 2001. URL http://dspace.mit.edu/handle/1721.1/8589.

[195] L. Sweeney. k-anonymity: A model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5):557–570, 2002.

[196] L. Tesfatsion. Agent-based computational economics: A constructive approach to economic theory. In *Handbook of Computational Economics, Volume 2*, pages 831–880. Elsevier, 2006. URL http://econ2.econ.iastate.edu/tesfatsi/hbintlt.pdf.

[197] A. D. Tuttle and D. K. Willimack. Privacy principles and data sharing: Implications of cipsea for economic survey respondents. Technical report, U.S. Census Bureau, 2005. URL http://www.fcsm.gov/05papers/Tuttle_Willimack_VB.pdf.

[198] R. E. Verrecchia. Essays on disclosure. *Journal of Accounting and Economics*, 32:97–180, 2001. URL http://www.sciencedirect.com/science/article/pii/S0165410101000258.

[199] W. E. Wagner. Administrative law, filter failure, and information capture. *Duke Law Review*, 59:1321–1432, 2010. URL http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1463&context=dlj.

[200] S. L. Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309):63–69, 1965.

[201] E. N. White. Lessons from the history of bank examination and supervision in the united states, 1863-2008. Technical report, Rutgers University, April 2009. URL http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2101709.

[202] White House. Freedom of information act. Technical report, The White House, January 2009. URL http://www.whitehouse.gov/the-press-office/freedom-information-act.

[203] O. E. Williamson. The theory of the firm as governance structure: From choice to contract. *Journal of Economic Perspectives*, 16(3):171–195, September 2002. doi: 10.1257/089533002760278776. URL http://www.aeaweb.org/articles.php?doi=10.1257/089533002760278776.

[204] R. C.-W. Wong, A. W.-C. Fu, K. Wang, and J. Pei. Minimality attack in privacy preserving data publishing. In *VLDB*, pages 543–554. VLDB Endowment, 2007.

[205] D. Xiao. Is privacy compatible with truthfulness? In R. D. Kleinberg, editor, *ITCS*, pages 67–86. ACM, 2013. ISBN 978-1-4503-1859-4. IACR eprint 2011/005.

[206] A. C. Yao. How to generate and exchange secrets. *In Proceedings of the 27th IEEE symposioum on Foundations of Computer science,pages 162-167*, 1986.

[207] A. O. Zarate and L. Zayatz. Essentials of the disclosure review process: A federal perspective. *Journal of Empirical Research on Human Research Ethics: An International Journal*, 1(3):51–62, September 2006. URL http://www.jstor.org/stable/10.1525/jer.2006.1.3.51.

[208] L. Zayatz. Disclosure avoidance practices and research at the u.s. census bureau: An update. Research Report Statistics 2005-06, U.S. Census Bureau, August 2005. URL http://www.census.gov/srd/papers/pdf/rrs2005-06.pdf.